INTRODUCTION TO NETWORKING ESSENTIALS AND TCP/IP

TCP/IP Course Outline

MSTP

- OSI Reference Model
- LAN Segmentation
- Internet Protocol Stack
- IP Addressing and Subnetting

Open Systems Interconnect (OSI)

MSTP

- OSI is a Layered Network Model for networking protocols. Establishes standards for internetworking.

- Allows for shortcut explanations to facilitate protocol comparisons.

- OSI is not a popular method for interconnecting computers. WHY? Seven layer stack is extremely complicated and next to impossible to keep track of for standardization purposes.

Why a layered Network Model?

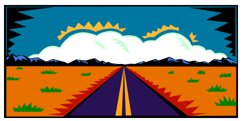
MSTP

- Clarify what general functions are to be done rather than how to do it.
- Reduce the complexity of networking into more manageable sub-layers.
- Enable interoperability using standard interfaces (Applicartion Programmable Interface).
- Allow changes in one layer to occur without changing other layers.
- Allows specialization within the network industry.

Physical and Logical Data Movement

MSTP

- <u>Physical movement of data</u>
  - Application layer protocol
    - Someone creates information on an application.
  - Communication protocol
    - The information is then packaged for transmission.
  - Transmission protocol
    - The package is now prepared for actual physical transmission.
- <u>Logical movement of data</u>
  - Physical topology
    - The data moves across some type of physical channel.



OSI Protocol Stack

MSTP

	Layer	Description
Application layer protocol	APPLICATION	•User interface: File, print, message, database, and application services.
	PRESENTATION	•How data is presented: Data translation
	SESSION	•Keeping data from different applications separate. Inter-host communication, dialog control.
Communication layer protocol	TRANSPORT	End-to-end connections. Reliable/Unreliable delivery
	NETWORK	•Routing; Logical addressing, which path to take
Physical topology	DATA LINK LLC/MAC)	•Framing; access to media
	PHYSICAL	•Physical topology. Binary transmission

Application Layer

MSTP

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK LLC/MAC)
PHYSICAL

- The application layer identifies and establishes the availability of intended communication partners.
- Synchronizes cooperating applications.
- Establishes agreement on procedures for error recovery and control of data integrity.

Application Layer cont...

MSTP

Network Applications

- Electronic Mail
- File Transfer
- Remote Access
- Client/Server Process
- Network Management
- Others

Internetwork Applications

- Electronic Data Interchange
- World Wide Web
- E-Mail Gateways
- Special-Interest Bulletin Boards
- Financial Transaction Services
- Internet Navigation Utilities
- Conferencing (Voice, Video, & Data)

Presentation Layer

MSTP

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK (LLC/MAC) PHYSICAL

- This layer ensures that information sent by the application layer of one system will be readable by the application layer of another.
    - Data translation
    - Encryption
    - Compression
- Negotiates data transfer syntax for the application layer.

Presentation Layer

MSTP

- **Graphics**
- **Visual Images**
  - **PICT**
  - **TIFF**
  - **JPEG**
  - **GIF**

- **Sound**
- **Video**
  - **MIDI**
  - **MPEG**
  - **QuickTime**

- **Text**
- **Data**
- **ASCII**

Capt Gaughen

Presentation Layer provides code conversion

Presentation Layer (Cont…)

MSTP

Session Layer

MSTP

- This layer establishes, manages, and terminates sessions between applications by offering three modes:
  - Simplex (monologue)
  - Half-duplex (forbidden interruption)
  - Full-duplex (flow control issue)
- Accomplished in three phases:
  - Connection establishment
  - Data transfer
  - Connection release
- Manages data exchange between presentation layer and entities.

Half-duplex and Full-duplex

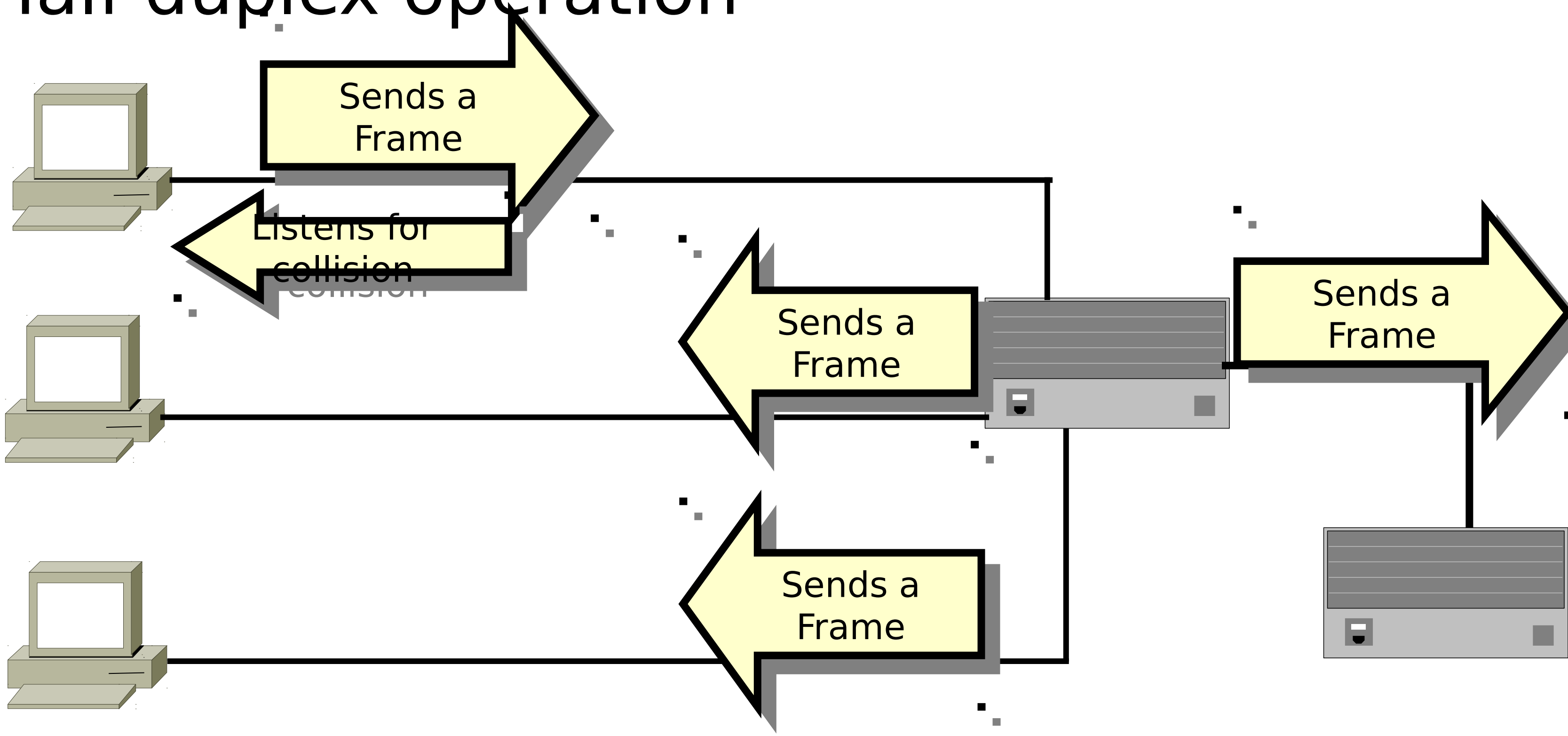
- Half-duplex – Nodes take turns transmitting and receiving. Ex. One way bridge

- Full-duplex – Nodes can transmit and receive simultaneously, but it requires a switch port, not a hub, to be able to do so.

Half Duplex

MSTP

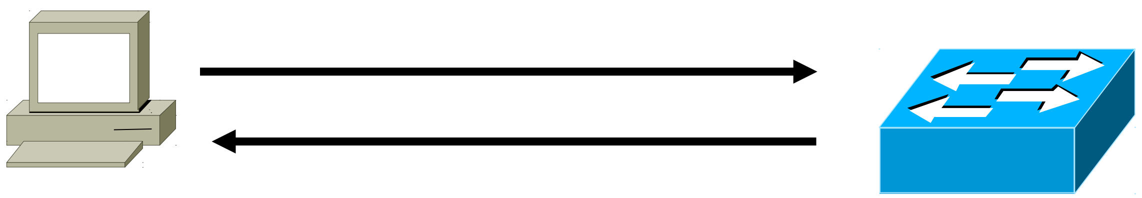
- Half-duplex operation



Full Duplex

MSTP

- Full duplex is allowed when the possibility of collision is removed.

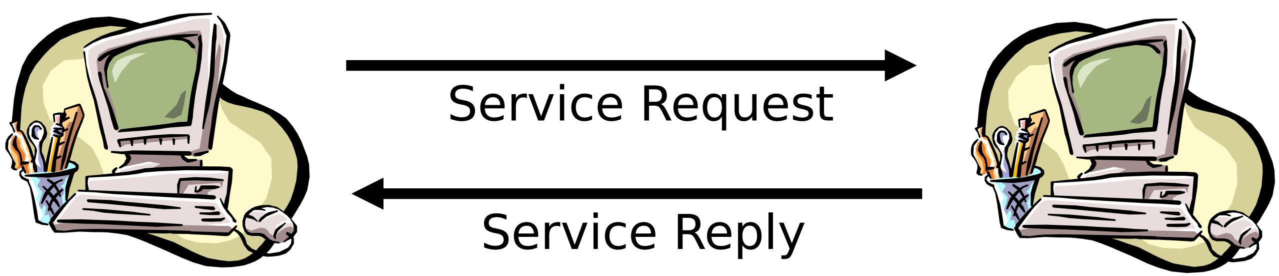


Because no collisions are possible, both ends can send and receive simultaneously. This reduces Ethernet congestion which results in low latency, information is moving in

Session-Layer Protocols and Interfaces

MSTP

- Network File System (NFS)
- Structured Query Language (SQL)
- Remote-Procedure Call (RPC)
- X Window System
- NetBios Names
- Internet Browsers
- DNA Session Control Protocol (SCP)



Transport Layer

MSTP

APPLICATION

PRESENTATION

SESSION

TRANSPOR
T

NETWORK

DATA LINK
PHYSICAL
LLC/MAC)

- Reliable network communication between end nodes
- Provides mechanisms for the establishment, maintenance, and termination of virtual circuits.
- Transport fault detection and recovery
- Information flow control (buffering,windowing, congestion avoidance)

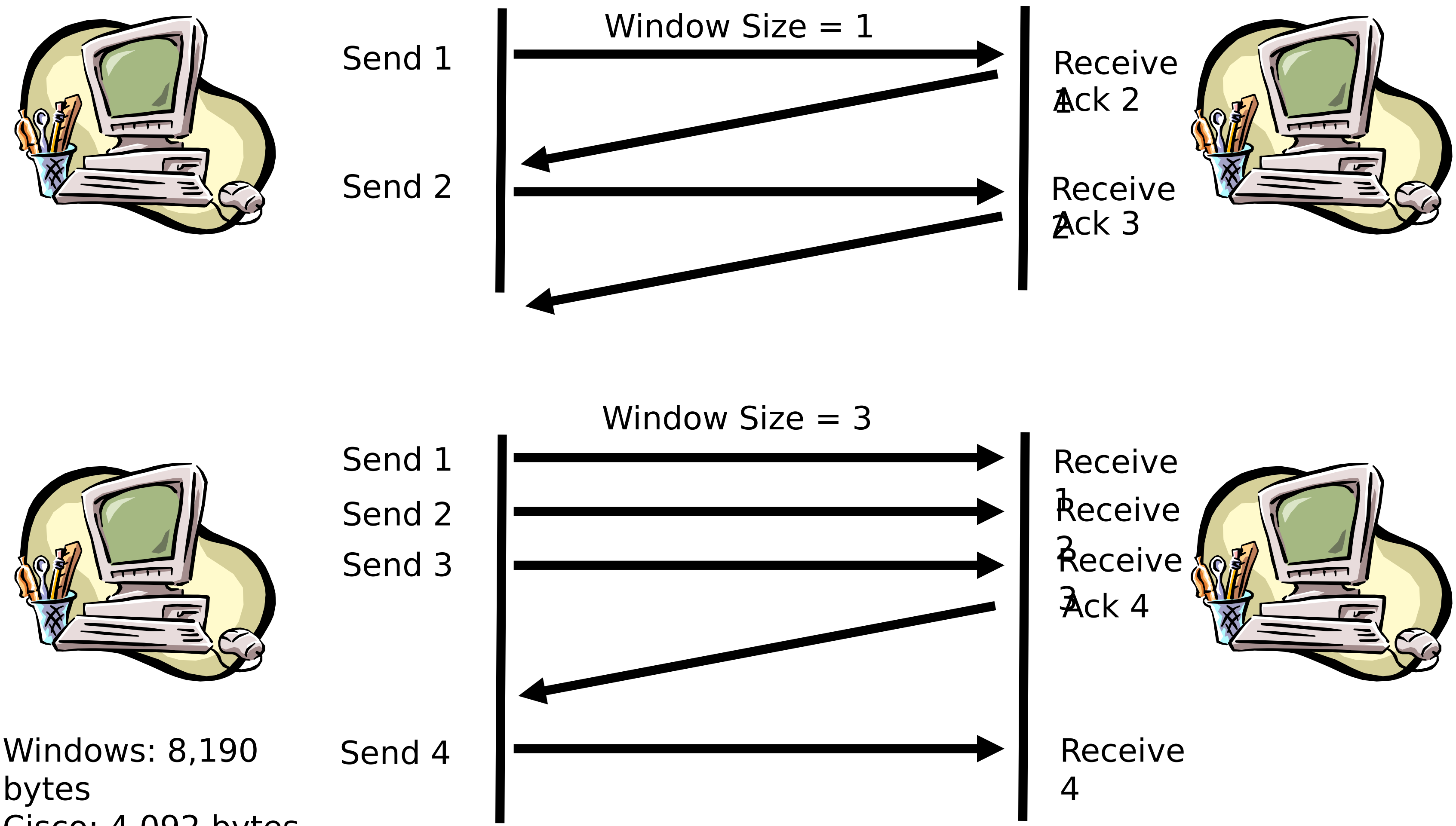
Buffering

MSTP

- Computers reserve enough buffer space that bursts of incoming data can be held until processed.
- Cannot slow down the transmission rate of the sender that is sending the data.
- Common method of dealing with the rate of arrival of data

Windowing

MSTP



Windows: 8,190 bytes
Cisco: 4,092 bytes

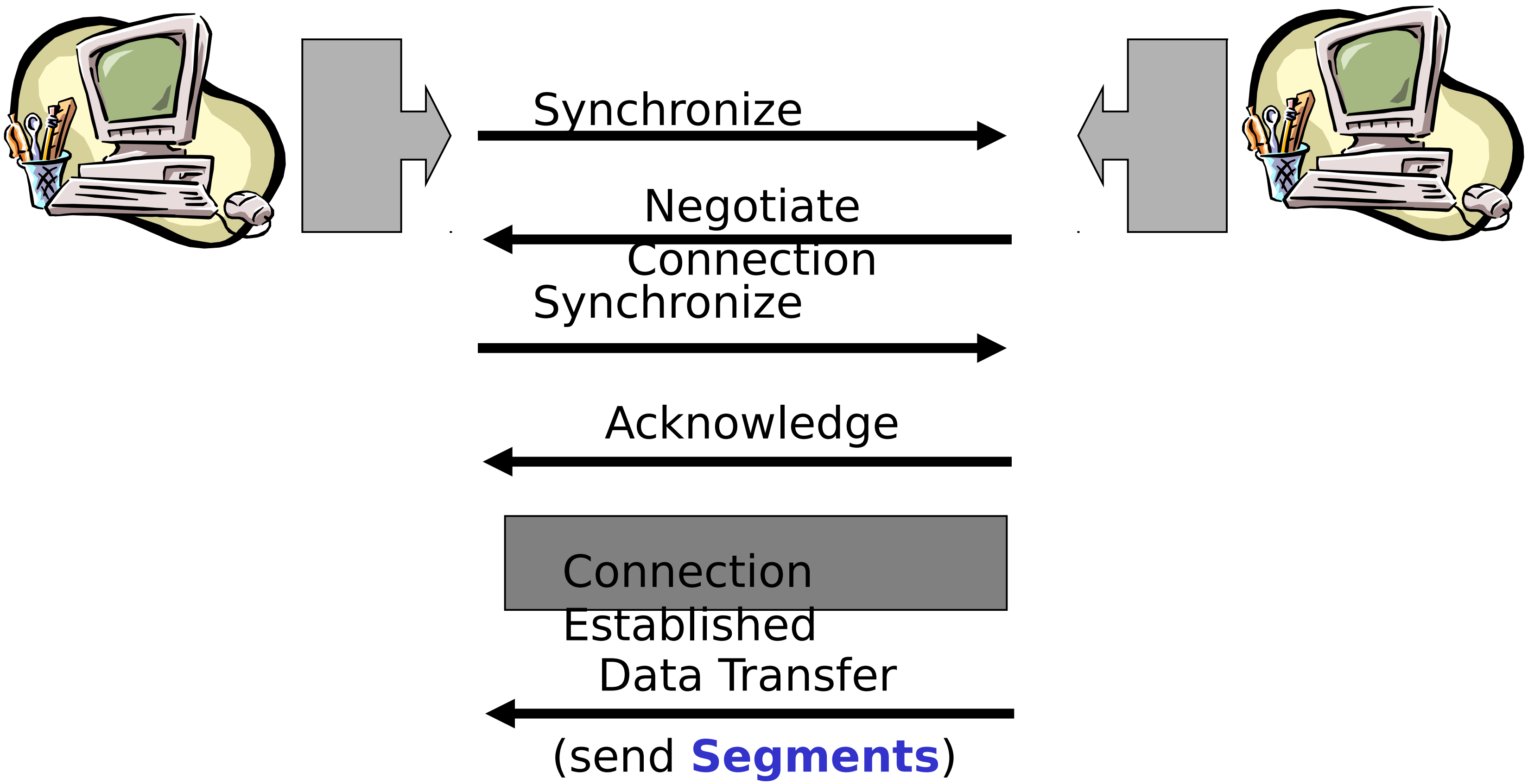
Congestion Avoidance

MSTP

- When a computer sees that its buffers are getting full, it sends a message to the sender to slow down sending messages.
- This process is used by Synchronous Data Link Control (SDLC) and Link Access Procedure, Balanced (LAPB) serial data link protocols.
- Ex. TCP/IP Internet Control Message Protocol (ICMP) message "Source Quench"
  - Sent by the receiver or some intermediate router to slow the sender. The sender will slow down gradually until "Source Quench"messages are no longer received.

Setting Up a Reliable Session

MSTP



Network Layer

MSTP

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK PHYSICAL LLC/MAC)

- The network layer is the layer at which routing occurs.
- This layer provides connectivity and path selection between two end systems.

Data Link

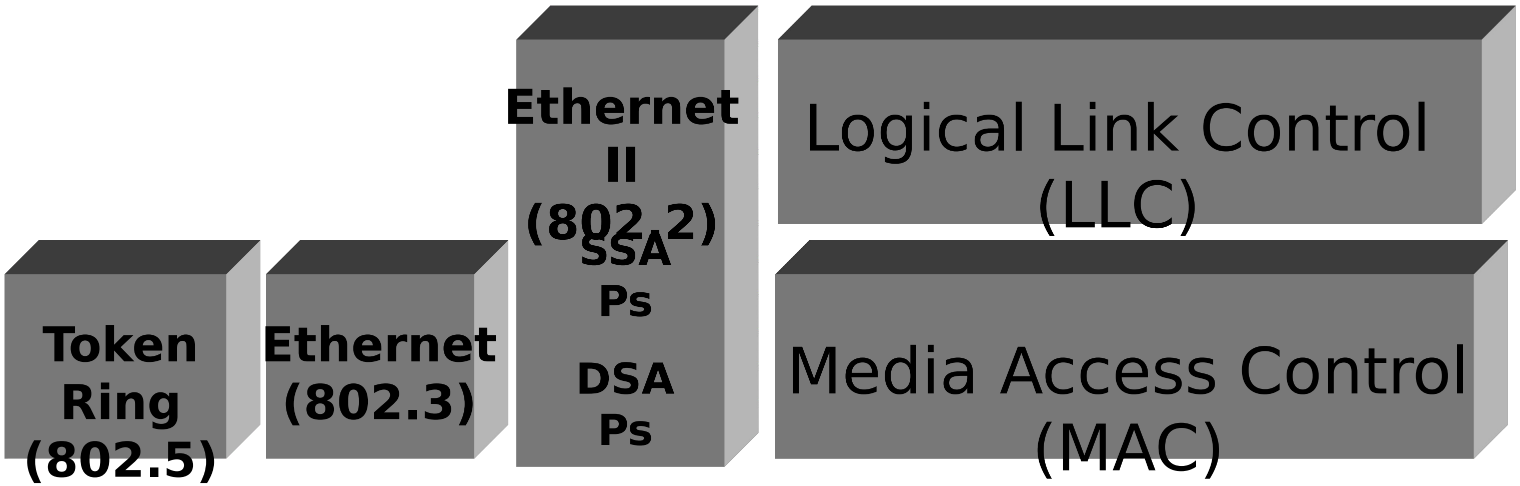
MSTP

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK (LLC/MAC) PHYSICAL

- This layer provides reliable transit of data across a physical link.
- Physical addressing (MAC)
- Network topology
- Line discipline (CSMA/CD & CSMA/CA)
- Error notification
- Divided into two sub-layers (MAC and LLC)

Data Link Sub-Layers

MSTP



- Logical Link Control acts as the managing buffer
  - Source Service Access Points (SSAPs)
  - Destination Service Access Points (DSAPs)

Data Link Sub-Layers

MSTP

Ethernet II (802.2)	**Preamble 8 Bytes**	**Dest Add 6 Bytes**	**Source Ad 6 Bytes**	**Type 2 Bytes**	**Data**	**Frame Check Sequence 4 Bytes**
Ethernet (802.3)	**Preamble 8 Bytes**	**Dest Add 6 Bytes**	**Source Ad 6 Bytes**	**Length 2 Bytes**	**Data**	**Frame Check Sequence 4 Bytes**

Physical Layer

MSTP

- The physical layer defines the electrical, mechanical, procedural and functional specifications for activating, maintaining, and deactivating the physical link between end systems.

Putting it all together …

MSTP

Data	Layer	Protocol Data Unit
	Application	
	Presentation	
Upper Layer Data	Session	
TCP Header / Upper Layer Data	Transport	Segment
IP Header / Data	Network	Packet
LLC Header / Data MAC Header / Data	Data Link	Frame
0101110101000111010	Physical	Bits

Devices at the different layers

MSTP

- OSI Model

Application
Presentation
Session
Transport
Network
Data Link
Physical

Routers
Switches
Hubs/Repeaters

LAN Segmentation & Networking Essentials

Internetworking Fundamentals

MSTP

- Internetworks are the communication structures that work to tie Local Area Networks (LAN) and Wide Area Networks (WAN) together.
- Primary goal is to move information anywhere quickly upon demand and with complete integrity.   Must be able to connect many different networks together to serve the organizations needs regardless of the type of physical media involved.

Internetworking Devices

MSTP

- LANs were designed to operate in limited geographical areas, such as one floor of a building, or a single building.
- LANs connect PCs together so that they can access network resources.
- A LAN connects physically adjacent devices on the network media or cable.
  - LAN Devices include: Repeaters, Bridges, Hubs, Switches, Routers, and Gateways.

Internetworking Devices Cont.

MSTP

- WANs extend beyond the LAN to connection networks located in different building, cities, states, and countries together.
- WANs are connected over ***serial*** lines.
  - WAN devices include: Routers, ATM Switches, X.25 and frame relay switches, modems, Channel Service Unit/Data Service Units (CSU/DSU), communication servers, and multiplexors.

Network Congestion

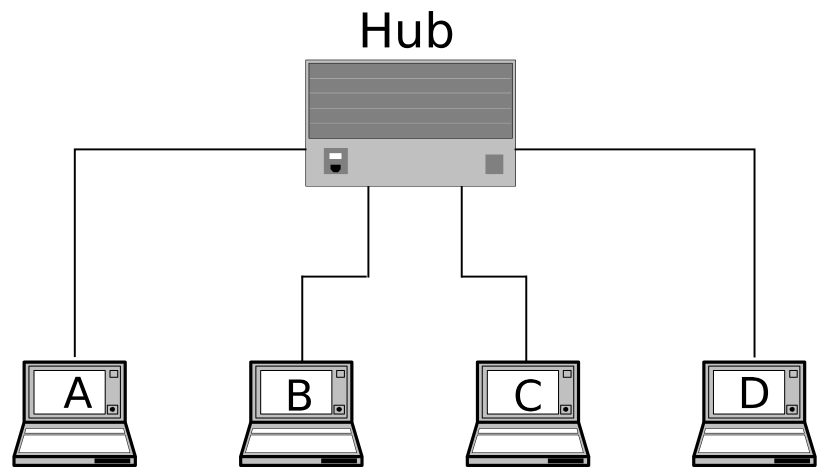
MSTP

- Where does it come from?
- How do I get rid of it?
  - Physical segmentation
  - Bridges
  - Routers
  - Switches

Hubs

MSTP

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK (LLC/MAC) Physical Layer



- All devices are in the same collision domain
- All devices are in the same broadcast domain
- All devices share the same bandwidth

Switches/Bridges

MSTP

APPLICATION

PRESENTATION

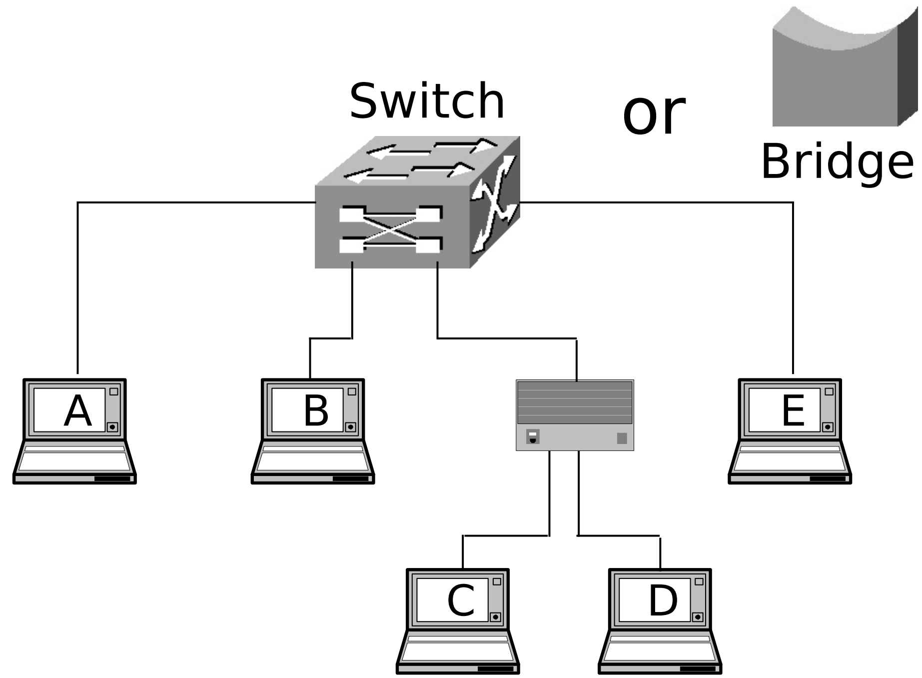
SESSION

TRANSPOR T

NETWORK

DATA LINK LLC/MAC)

Physical Layer



•Each Segment has its own collision domain

•All segments are in the same broadcast domain

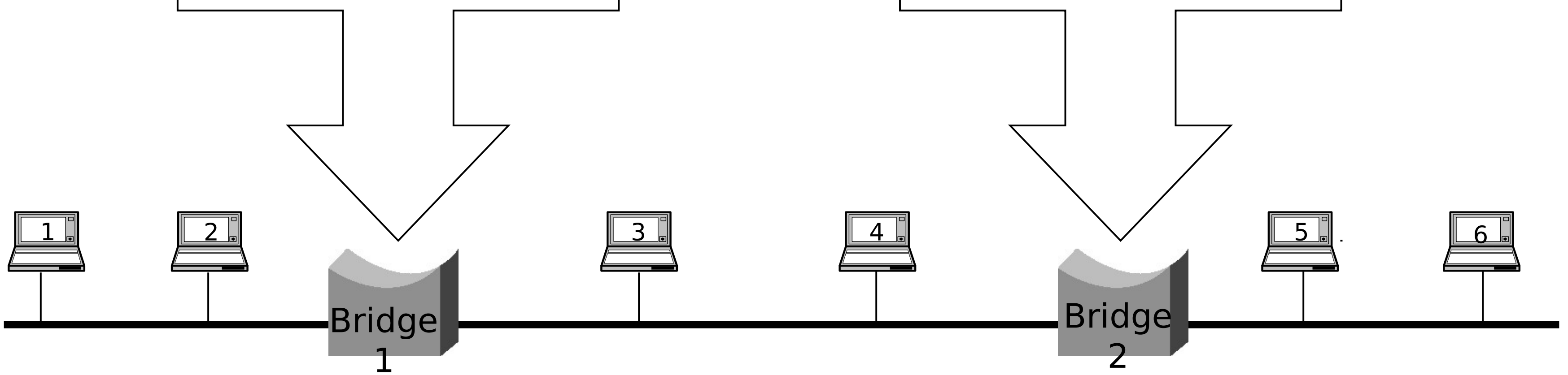
•Listening, Learning, Filtering and

Segmentation with Bridges

MSTP

Forwarding Table	
Host	Segments
1	1
2	1
3	2
4	2
5	2
6	2

Forwarding Table	
Host	Segments
1	2
2	2
3	2
4	2
5	3
6	3



Segment 1 Segment 2 Segment 3

Routers

MSTP

APPLICATION

PRESENTATION

SESSION

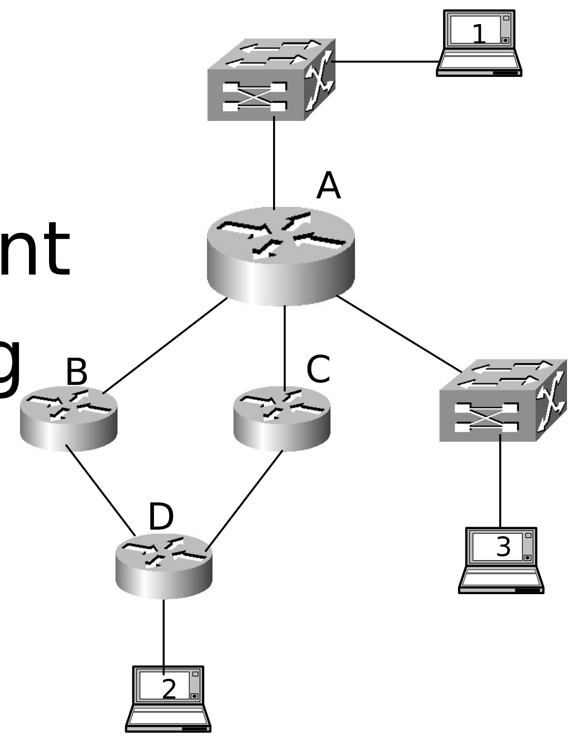
TRANSPORT

NETWORK

DATA LINK (LLC/MAC)

Physical Layer

- Broadcast control
- Multicast control
- Optimal path determination
- Traffic Management
- Logical addressing
- Connects to WAN services



Ethernet: Collisions

MSTP

- Certain level of collisions are expected on CSMA/CD LANs
- Excessive collisions can result from faulty components or overloaded segments
  - **Bad or excessively long cables**
  - **Bad NICs or transceivers**
- Establishing a baseline is helpful to determine normal levels
- Local collisions
  - **Occur on local LAN segment**
  - **Detected by circuitry in LAN interfaces**
- Remote collisions
  - **Occur on other side of repeater nodes**

CSMA/CD

MSTP

1. Sender is ready to send the frame. It listens to detect whether any frame is currently being received.
2. If Ethernet is silent, the devices begins to send the frame.
3. The sending device begins to listen to ensure that the frame it is sending does not collide with a frame that another station is sending.
4. If no collision occurs, the bits of the sent frame are received back successfully.

5 If a collision occurred, the device sends a jam signal and then waits a random amount of time before repeating the process.

Ethernet: Jabber

MSTP

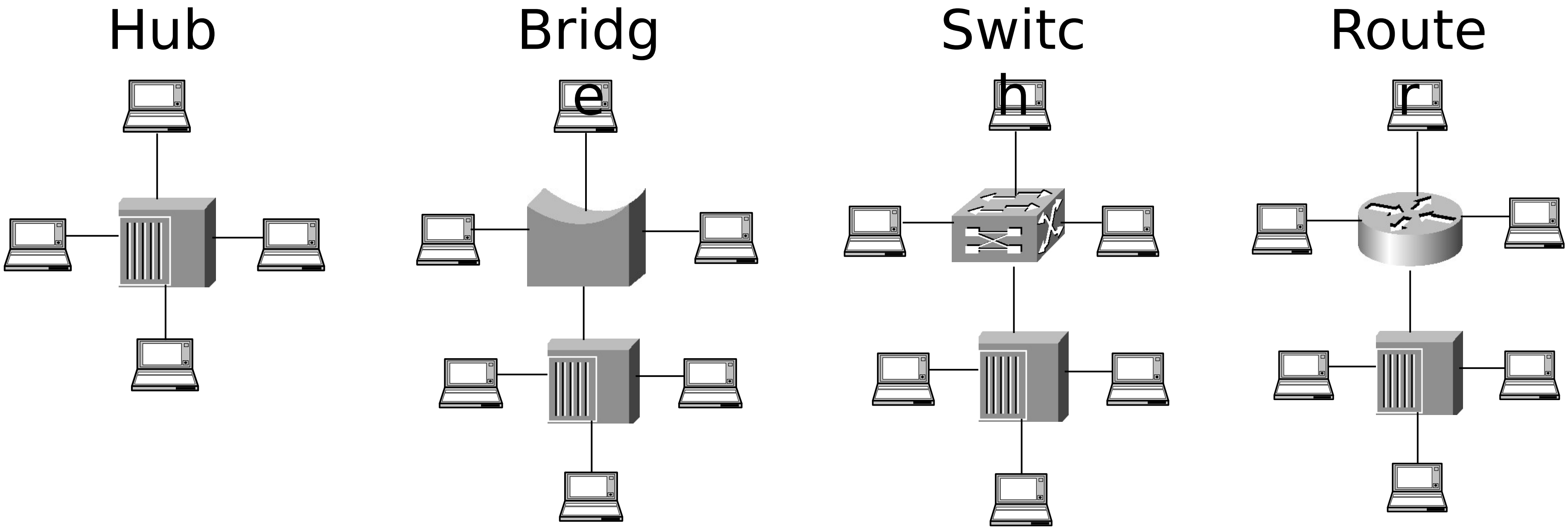
- Jabber
  - Frames are longer than 1518 bytes
  - Fails CRC check
- Causes
  - Caused by faulty transceivers
  - Transceivers can transmit for only 150-millisecond intervals
    - Sufficient time to transmit 1518 bytes
  - If transceiver does not stop after 1518 bytes, jabber results

Ethernet: Performance Issues

- Measuring network utilization
  - Protocol analyzers
  - User complaints
  - Rule of thumb: shared Ethernet segments < 40% utilization
- Improving network utilization
  - Segmenting with routers
  - Segmenting with switches

Creating Domains

MSTP



Collision Domains: 1 4 4

4

Broadcasts Domains: 1 1 1

4

TCP/IP Protocol Stack

TCP/IP: What and Why?

MSTP

- **What is TCP/IP?**
  - TCP/IP is the basic network protocol that is used as the base language for Joint Service and commercial worldwide communications . Think of it as the "body language" of network protocols, meaning that it is known worldwide as a basic means of communicating.
- **Why do we care about it?**
  - Marine Corps tactical systems talk in native IP.

What is TCP/IP...continued

MSTP

- TCP/IP is not a single protocol, but rather, a suite of protocols that work together to interconnect networks and provide a wide variety of services.

- Basic functions of TCP/IP are **remote login, file transfer, and email**. TCP/IP enables network devices to determine the physical address of LAN nodes, to map English language names to numeric machines names, and to manage the network.

- Protocols were created to work with virtually any host hardware, operating system and connecting media. Networks built upon TCP/IP

TCP/IP Timeline

MSTP

- ARPANET begins with 3 computers in California and one in Utah
- MID 1970's - DARPA researching packet switching technology. DARPA funded research of internetworking technology
- 1977 - 1979 - TCP/IP Standards defined (1969 - First work on protocol)
- 1980 - DARPA began converting research nets to TCP/IP
University of California (Berkeley) distributes BSD UNIX. DARPA funds UCB to integrate TCP/IP into UNIX
TCP/IP on ARPANET and majority of college networks
- 1983 - OSD mandated TCP/IP for "all" long haul networks.
DOD adopts TCP/IP as standard. ARPANET divides

TCP and IP

MSTP

- TCP
  - Connection Oriented
  - Requires Synchronization
    - Synchronization lost - reset session
  - Requires ACK
  - Sequencing numbers
    - No ACK - retransmit
    - Bad segment - retransmit all
  - Data Flow Control
    - Windowing

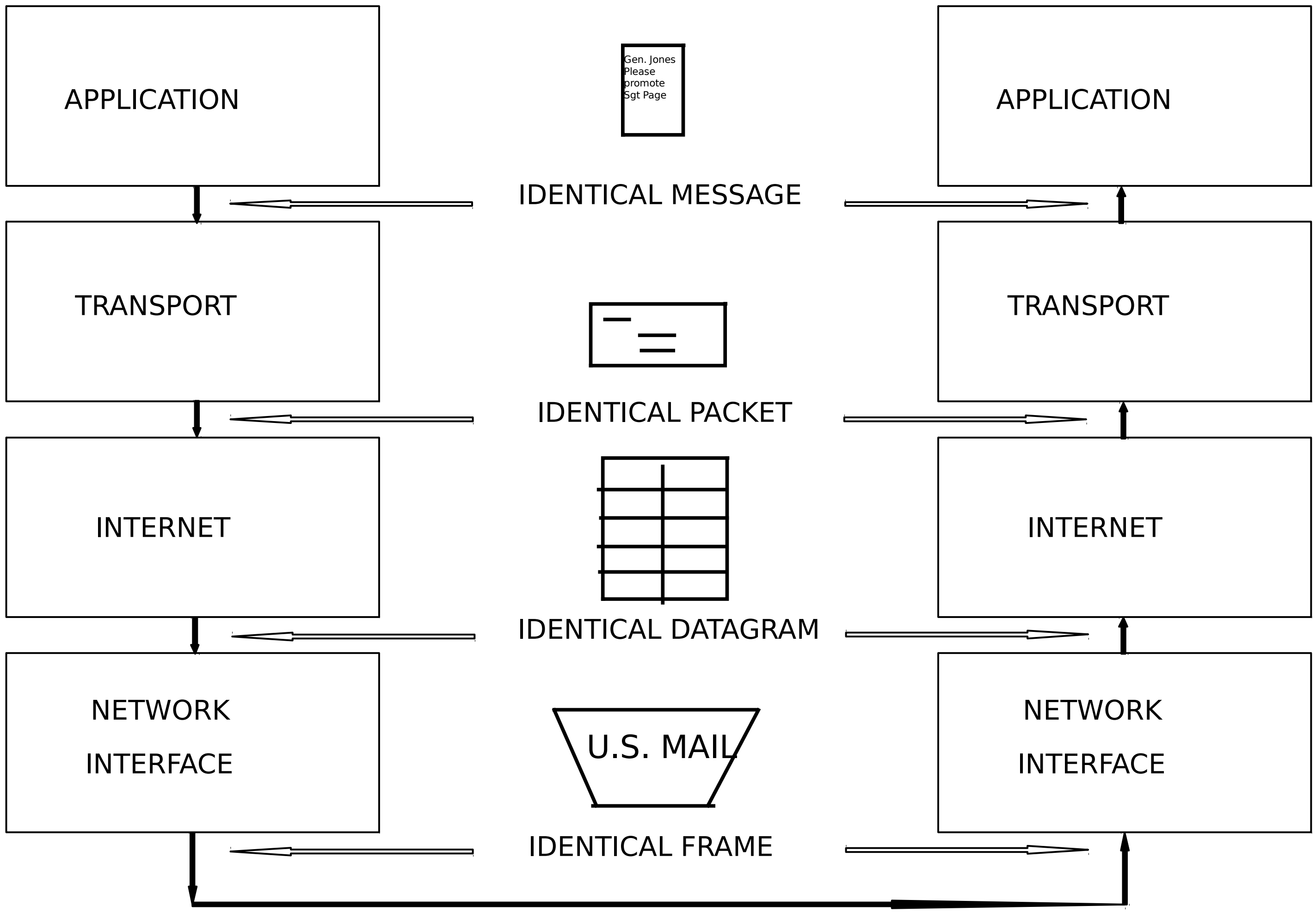
- IP:
  - Unreliable, “best effort”
    - No ACK required
    - No guarantee of delivery
      - Packets could get lost
      - Delivered out of sequence
      - Duplicated
      - Delayed

OSI to TCP/IP Comparison

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>APPLICATION</td><td rowspan="3">PROCESS / APPLICATION</td></tr>
<tr><td>PRESENTATION</td></tr>
<tr><td>SESSION</td></tr>
<tr><td>TRANSPORT</td><td>TRANSPORT (HOST-TO-HOST)</td></tr>
<tr><td>NETWORK</td><td>INTERNET</td></tr>
<tr><td>DATA LINK</td><td rowspan="2">NETWORK ACCESS</td></tr>
<tr><td>PHYSICAL</td></tr>
</table>

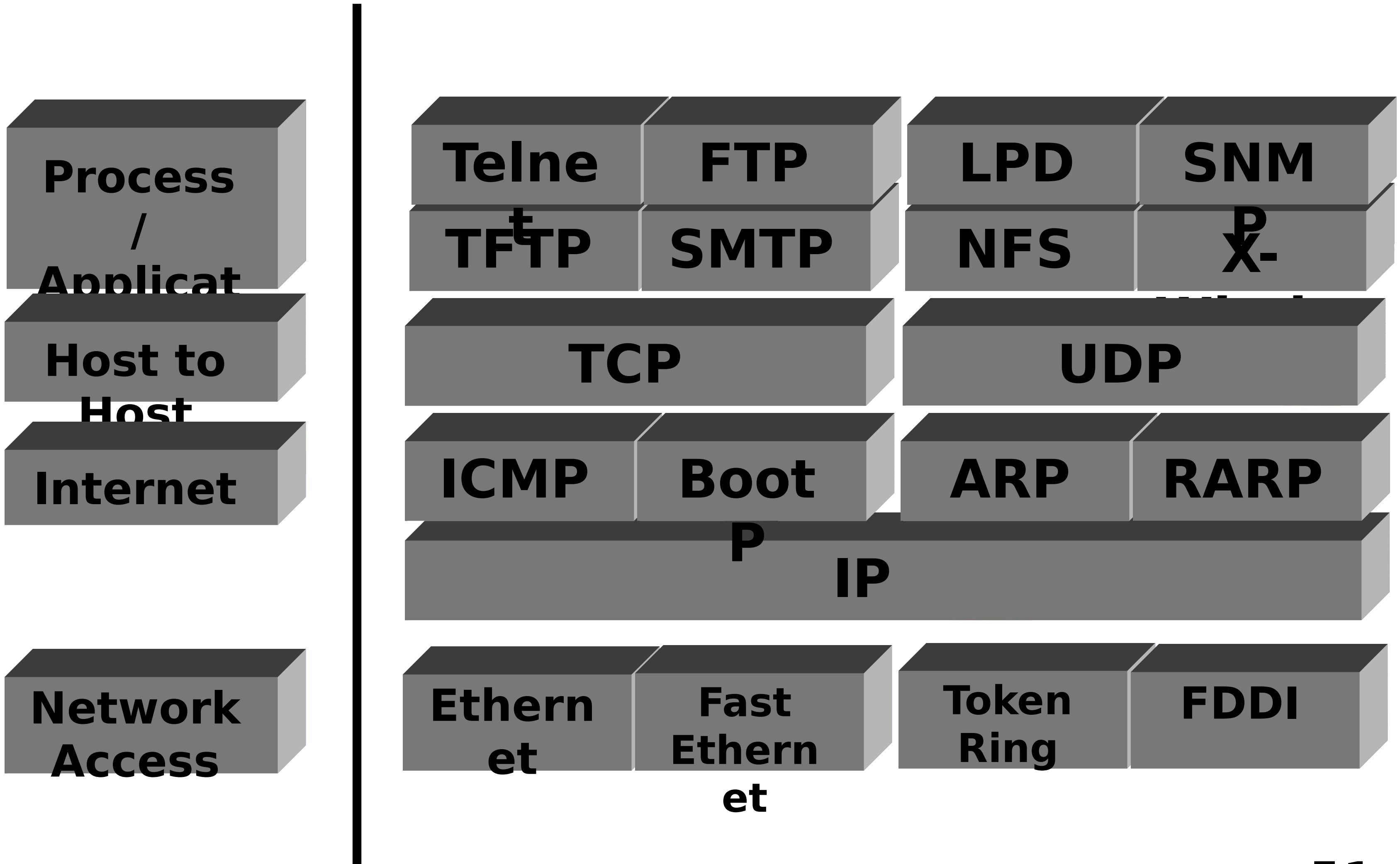
TCP/IP Protocol Stack

MSTP



TCP/IP Protocol Stack

MSTP



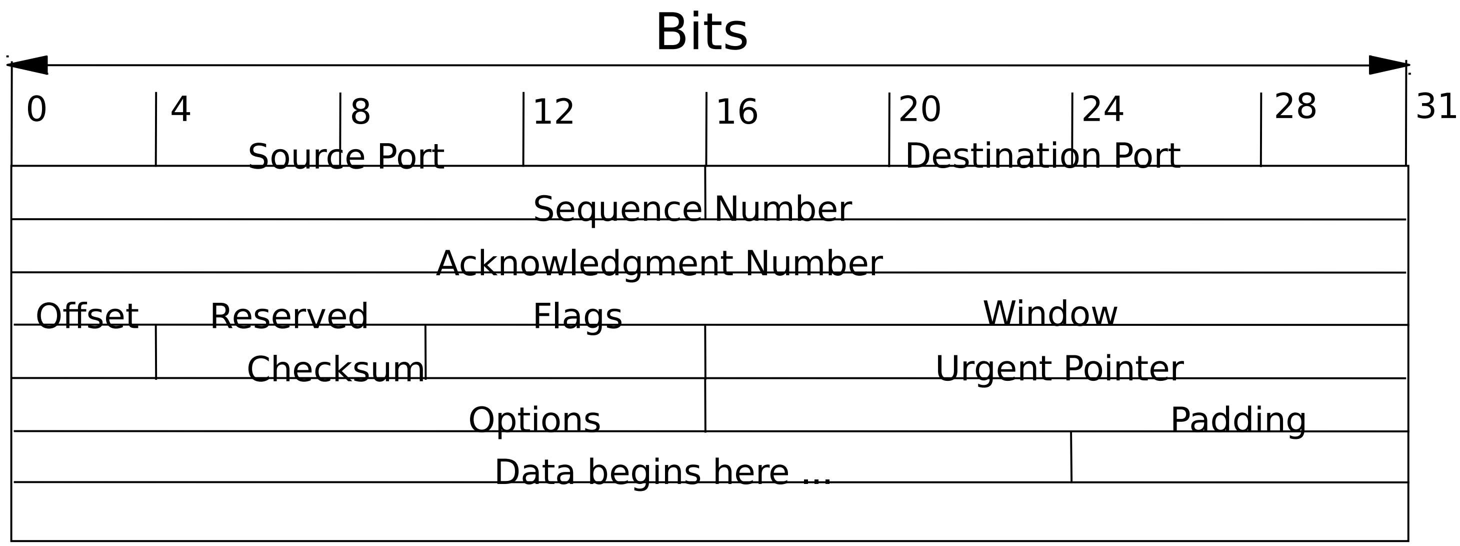
Transmission Control Protocol (TCP)

MSTP

- Connection oriented
  - Connection must be established prior to data transfer
  - Adds overhead
- In sequence delivery
  - Uses segment numbers to guarantee packet arrival in sequence deliver
  - Adds error checking & sequence numbering
- Provides graceful release
  - Ensures all data sent is received
- Reliable
  - Acknowledgment of received packets

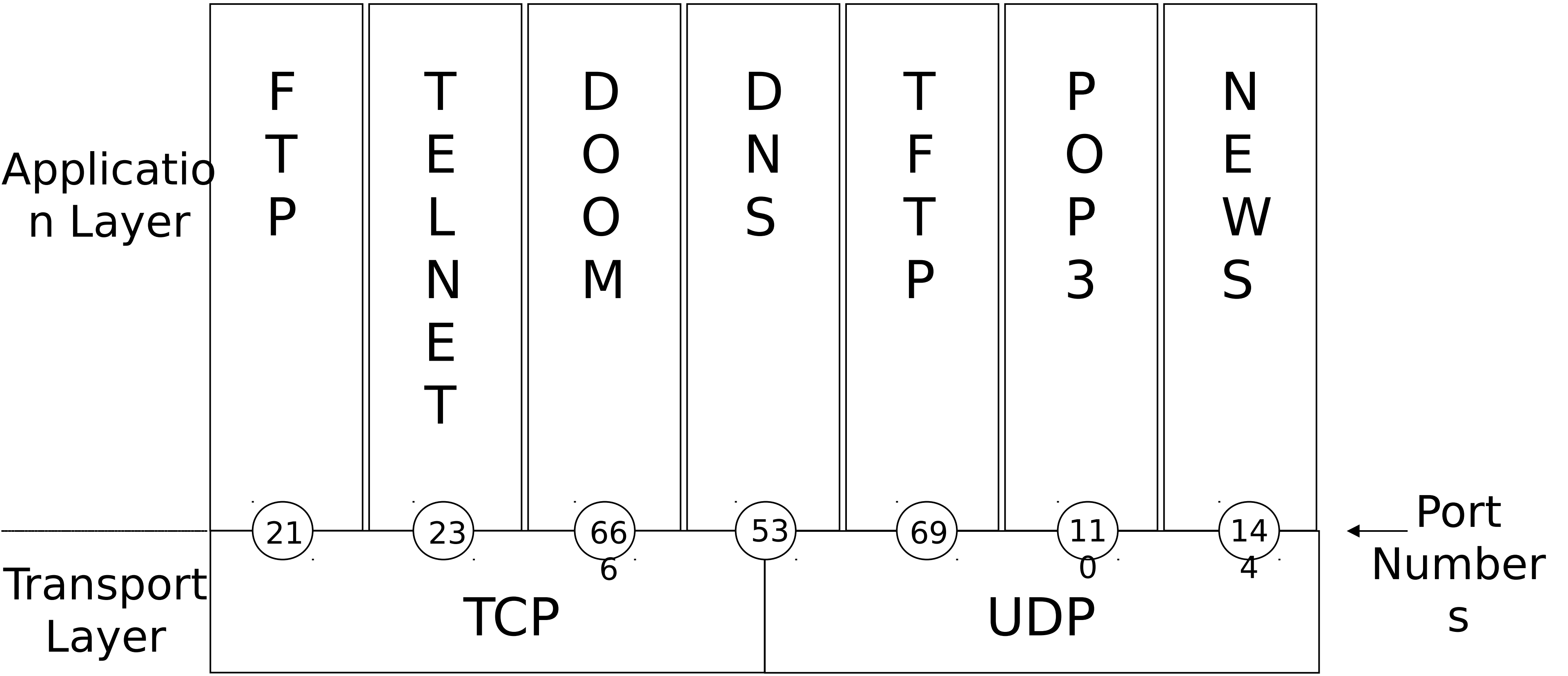
TCP Header

MSTP



TCP/UDP Port Examples

MSTP



Port Number

- 0 – 255 are assigned to public applications
    - 80 is assigned for HTTP
- 256 – 1023 are assigned to “well known sockets”
    - 1752 is assigned for VTC
- 1024 and up are used to set up sessions
    - Randomly assigned

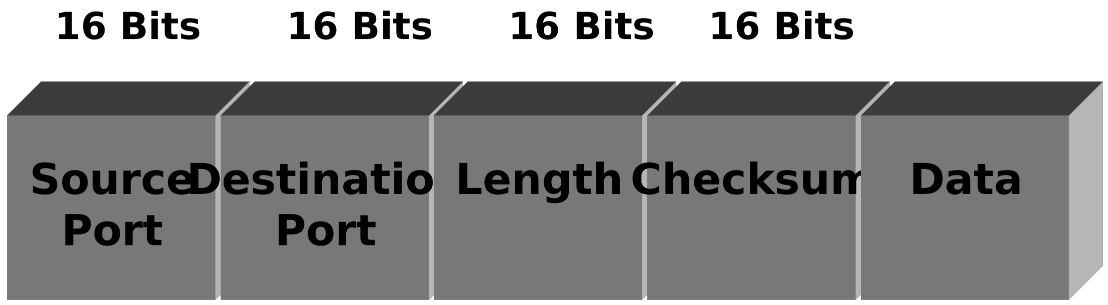
User Datagram Protocol (UDP)

MSTP

- Used when all data fits in one packet
  - SNMP (Simple Network Management Protocol)
  - DNR (Domain Name Resolver)
  - NBT (NetBIOS over TCP/IP)
- Unreliable
  - No acknowledgment at this layer
- User data integrity
  - Adds header and computes checksum
- Why use UDP?
  - Lower overhead
  - Small amount of data for transmission
  - Less overhead to retransmit if data lost
  - Application entity has its own reliability built in

UDP Header

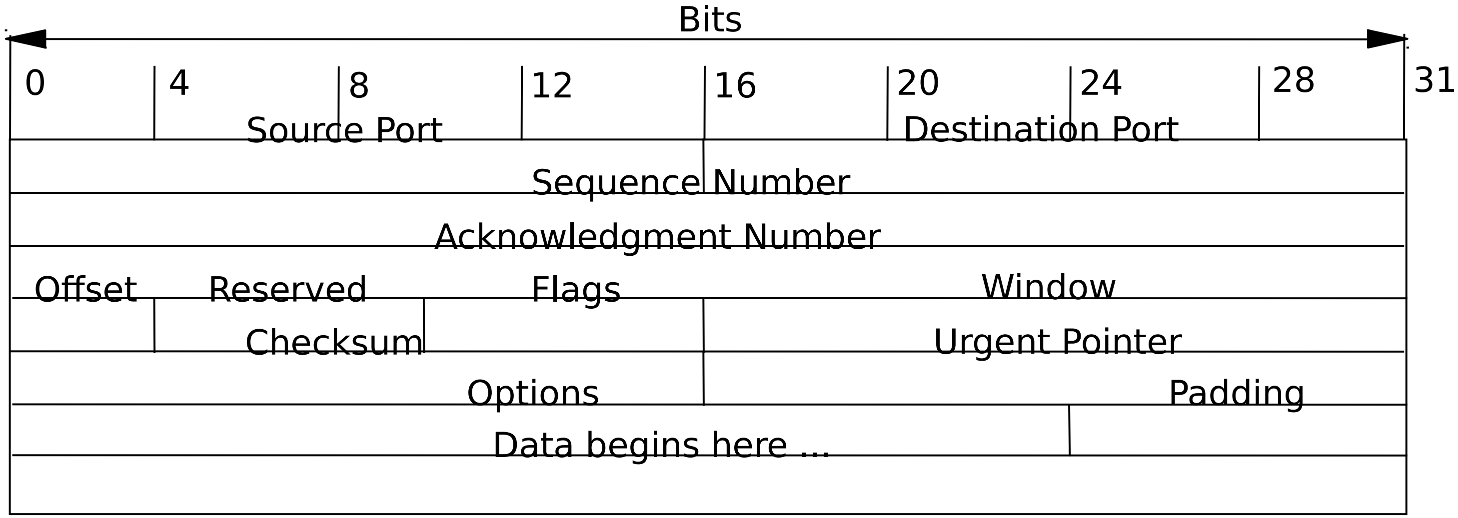
MSTP



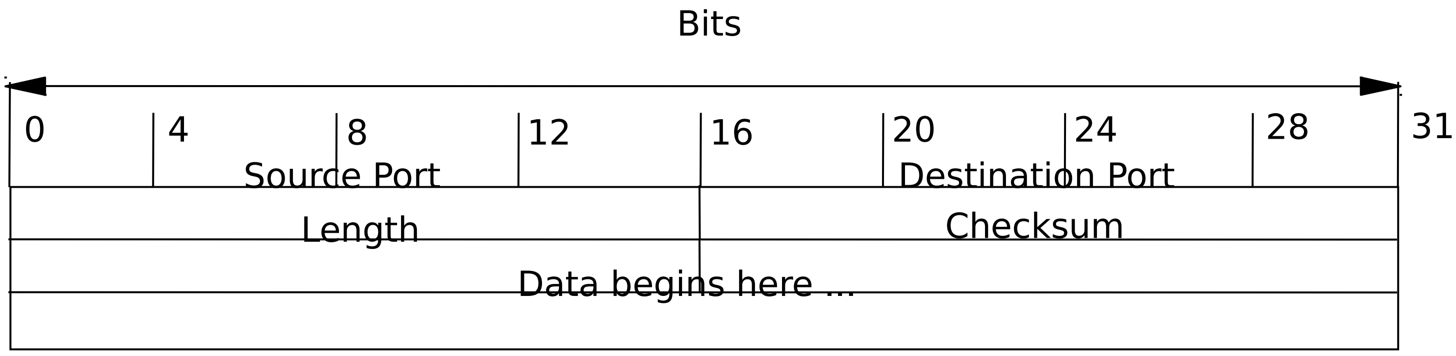
TCP vs. UDP Header

MSTP

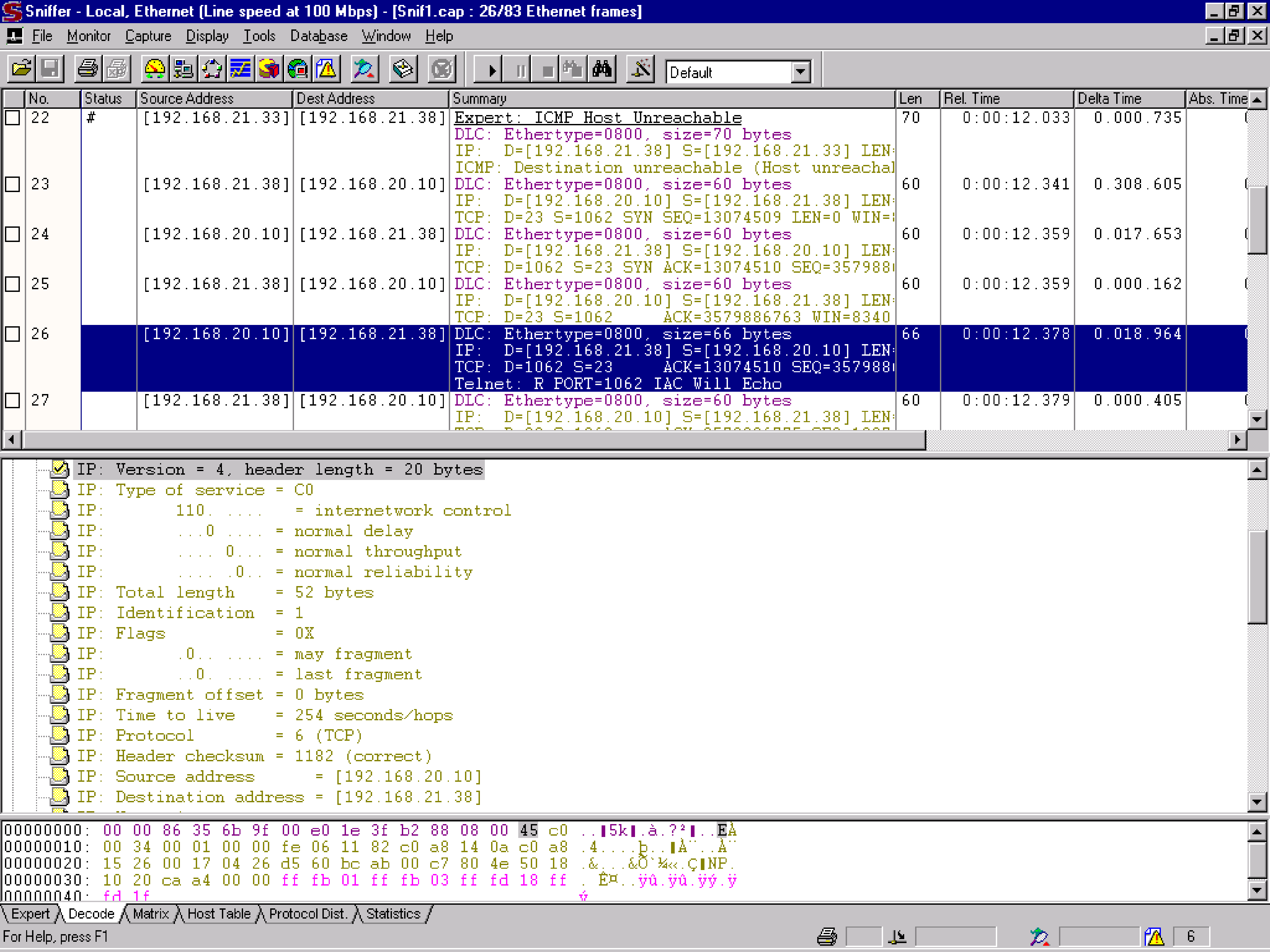
TCP Header



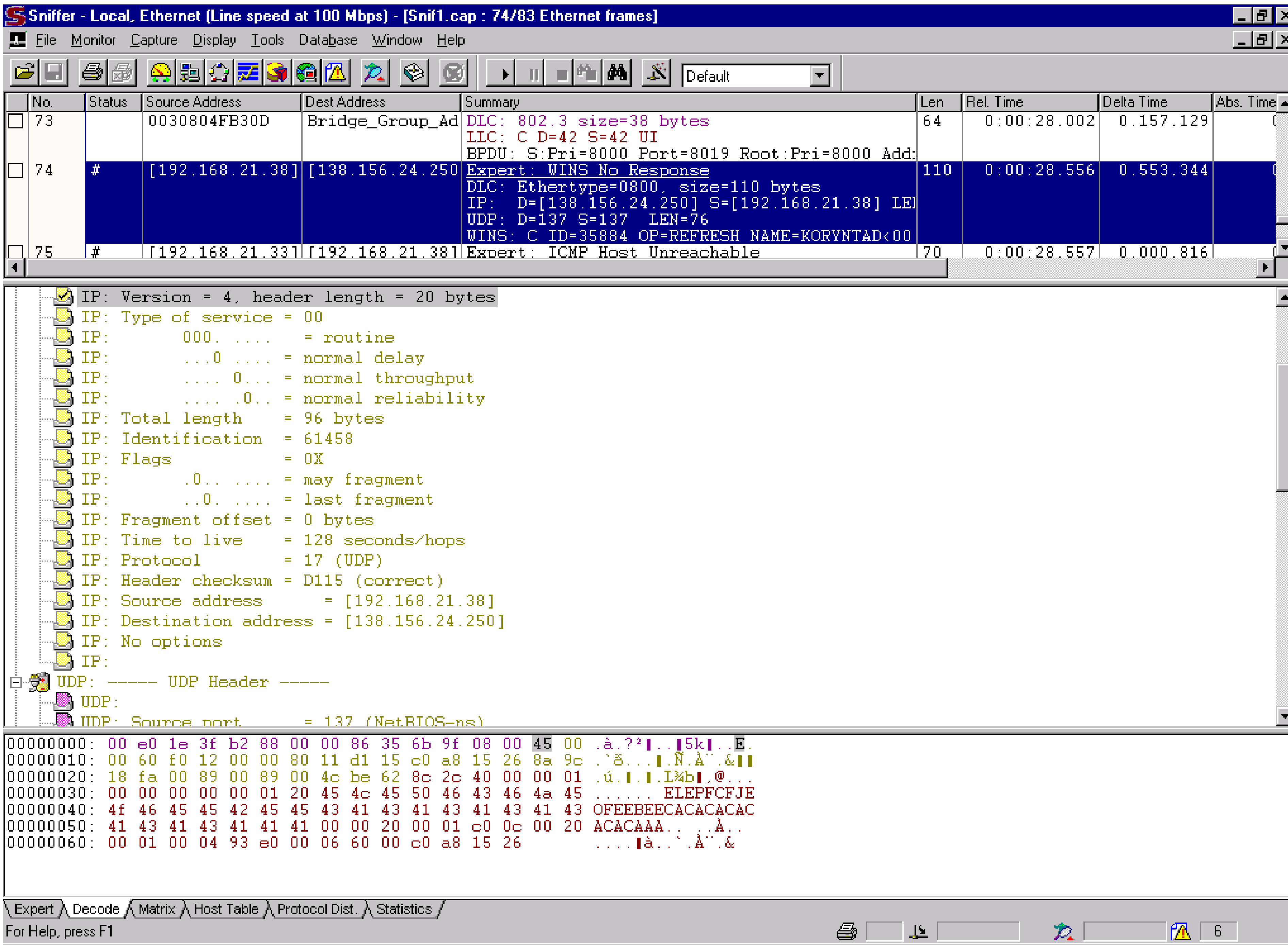
UDP Header




Bring out the Sniffer

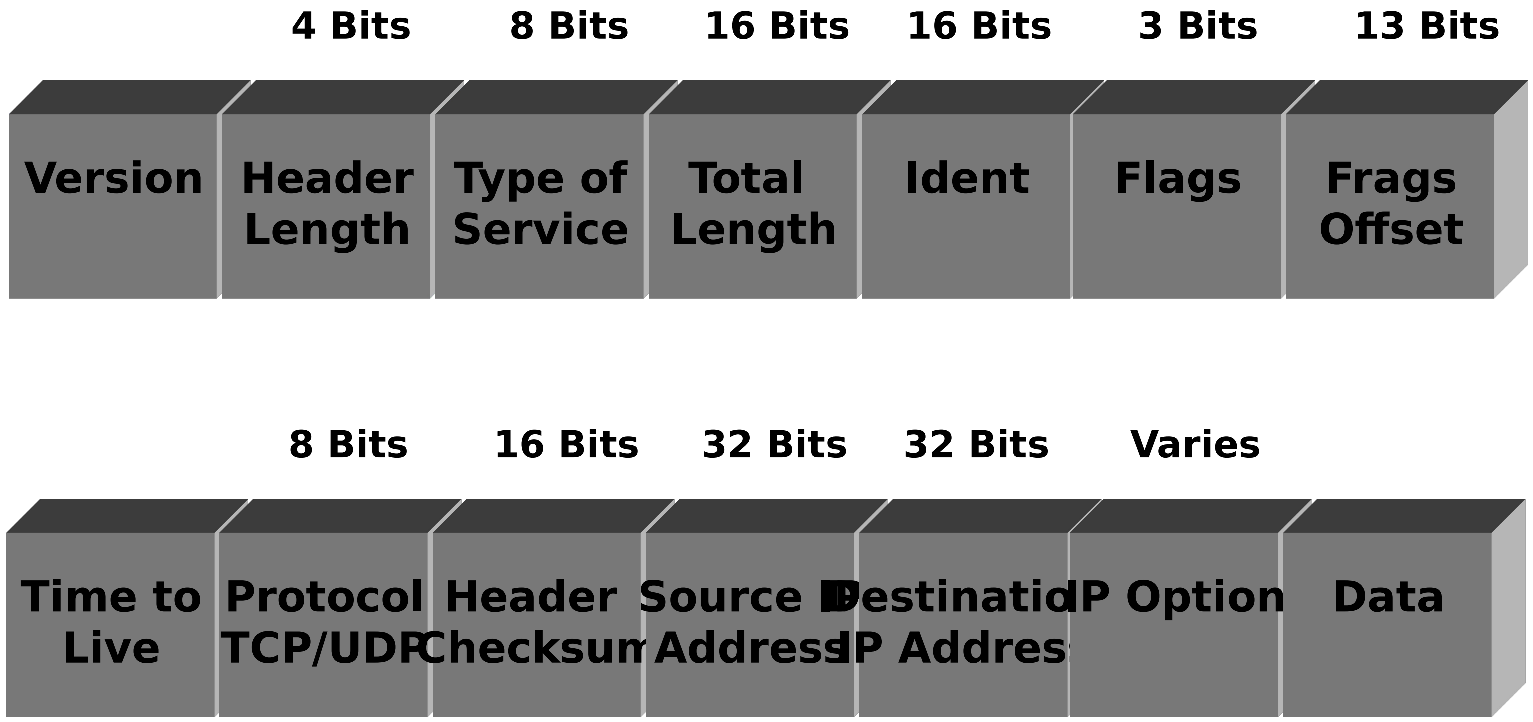


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Snif1.cap : 26/83 Ethernet frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len Rel. Time Delta Time Abs. Time
22 # [192.168.21.33] [192.168.21.38] Expert: ICMP Host Unreachable 70 0:00:12.033 0.000.735
DLC: Ethertype=0800, size=70 bytes
IP: D=[192.168.21.38] S=[192.168.21.33] LEN
ICMP: Destination unreachable (Host unreacha
23 [192.168.21.38] [192.168.20.10] DLC: Ethertype=0800, size=60 bytes 60 0:00:12.341 0.308.605
IP: D=[192.168.20.10] S=[192.168.21.38] LEN
TCP: D=23 S=1062 SYN SEQ=13074509 LEN=0 WIN=
24 [192.168.20.10] [192.168.21.38] DLC: Ethertype=0800, size=60 bytes 60 0:00:12.359 0.017.653
IP: D=[192.168.21.38] S=[192.168.20.10] LEN
TCP: D=1062 S=23 SYN ACK=13074510 SEQ=357988
25 [192.168.21.38] [192.168.20.10] DLC: Ethertype=0800, size=60 bytes 60 0:00:12.359 0.000.162
IP: D=[192.168.20.10] S=[192.168.21.38] LEN
TCP: D=23 S=1062 ACK=3579886763 WIN=8340
26 [192.168.20.10] [192.168.21.38] DLC: Ethertype=0800, size=66 bytes 66 0:00:12.378 0.018.964
IP: D=[192.168.21.38] S=[192.168.20.10] LEN
TCP: D=1062 S=23 ACK=13074510 SEQ=357988
Telnet: R PORT=1062 IAC Will Echo
27 [192.168.21.38] [192.168.20.10] DLC: Ethertype=0800, size=60 bytes 60 0:00:12.379 0.000.405
IP: D=[192.168.20.10] S=[192.168.21.38] LEN
IP: Version = 4, header length = 20 bytes
IP: Type of service = C0
IP: 110. .... = internetwork control
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: Total length = 52 bytes
IP: Identification = 1
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 254 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 1182 (correct)
IP: Source address = [192.168.20.10]
IP: Destination address = [192.168.21.38]
00000000: 00 00 86 35 6b 9f 00 e0 1e 3f b2 88 08 00 45 c0
00000010: 00 34 00 01 00 00 fe 06 11 82 c0 a8 14 0a c0 a8
00000020: 15 26 00 17 04 26 d5 60 bc ab 00 c7 80 4e 50 18
00000030: 10 20 ca a4 00 00 ff fb 01 ff fb 03 ff fd 18 ff
00000040: fd 1f
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
6


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Snif1.cap : 74/83 Ethernet frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len Rel. Time Delta Time Abs. Time
73 0030804FB30D Bridge_Group_Ad DLC: 802.3 size=38 bytes 64 0:00:28.002 0.157.129
LLC: C D=42 S=42 UI
BPDU: S:Pri=8000 Port=8019 Root:Pri=8000 Add:
74 # [192.168.21.38] [138.156.24.250 Expert: WINS No Response 110 0:00:28.556 0.553.344
DLC: Ethertype=0800, size=110 bytes
IP: D=[138.156.24.250] S=[192.168.21.38] LE
UDP: D=137 S=137 LEN=76
WINS: C ID=35884 OP=REFRESH NAME=KORYNTAD<00
75 # [192.168.21.33] [192.168.21.38] Expert: ICMP Host Unreachable 70 0:00:28.557 0.000.816
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: Total length = 96 bytes
IP: Identification = 61458
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = D115 (correct)
IP: Source address = [192.168.21.38]
IP: Destination address = [138.156.24.250]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 137 (NetBIOS-ns)
00000000: 00 e0 1e 3f b2 88 00 00 86 35 6b 9f 08 00 45 00
00000010: 00 60 f0 12 00 00 80 11 d1 15 c0 a8 15 26 8a 9c
00000020: 18 fa 00 89 00 89 00 4c be 62 8c 2c 40 00 00 01
00000030: 00 00 00 00 00 01 20 45 4c 45 50 46 43 46 4a 45 ...... ELEPFCFJE
00000040: 4f 46 45 45 42 45 45 43 41 43 41 43 41 43 41 43 OFEEBEECACACACAC
00000050: 41 43 41 43 41 41 41 00 00 20 00 01 c0 0c 00 20 ACACAAA.. ..À..
00000060: 00 01 00 04 93 e0 00 06 60 00 c0 a8 15 26
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
6

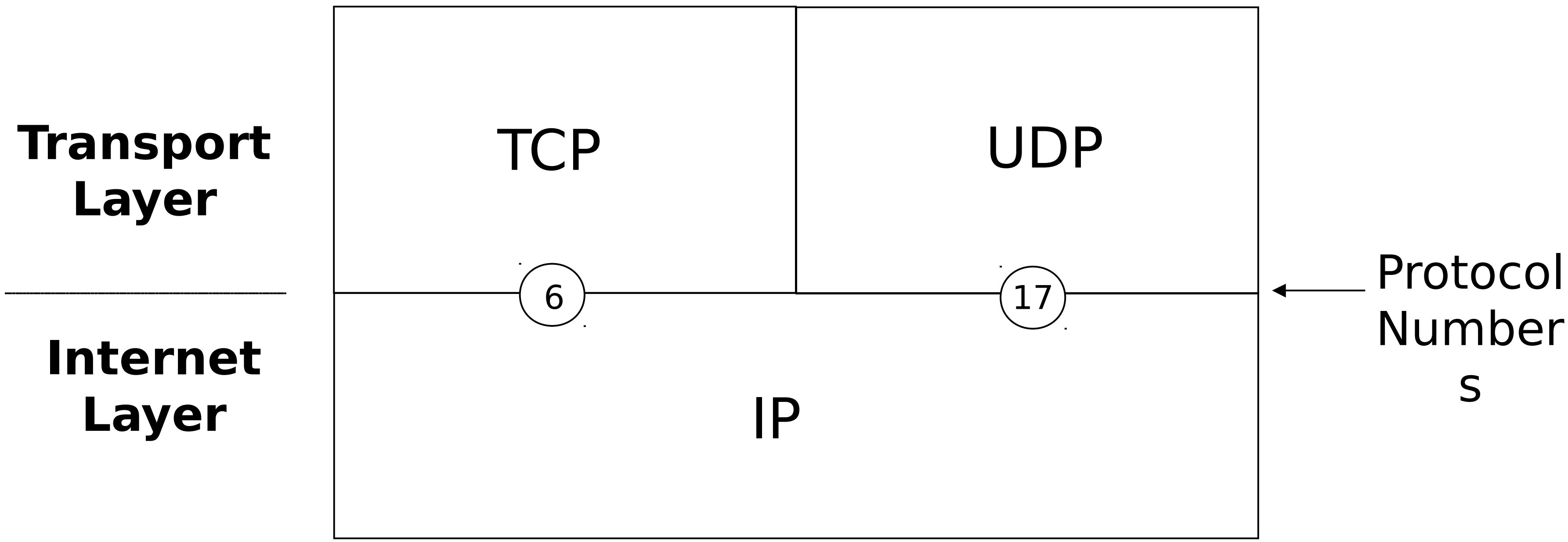
IP Header

MSTP



IP Port has to be either

MSTP



Data Encapsulation

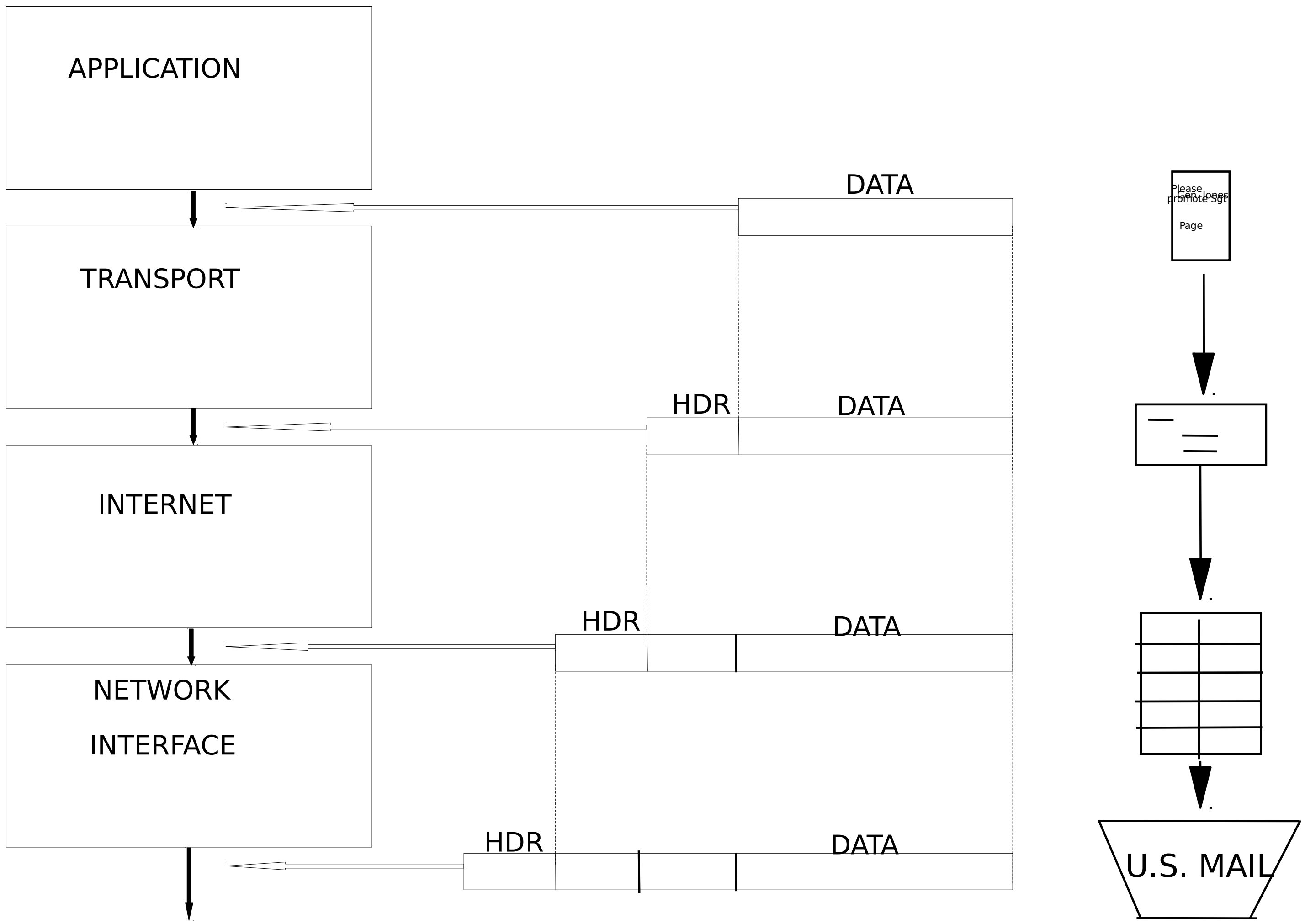
MSTP

Gen. Smith writes original letter on piece of paper .

Maj. Bill puts the letter into an envelope.

Sgt York places the envelope into a guard mail package.

Pvt. Session throws the guard mail into his mail bag.



How the computer sees the layers

MSTP

APPLICATION LAYER

PROGRAM RUN BY USER

TRANSPORT LAYER

CONNECTION ORIENTED
NON CONNECTION ORIENTED

INTERNET LAYER

NETWORK ADDRESS

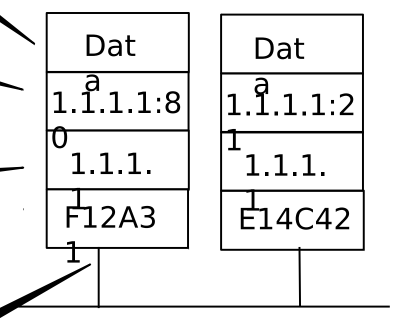
IP ADDRESS

NETWORK INTERFACE LAYER

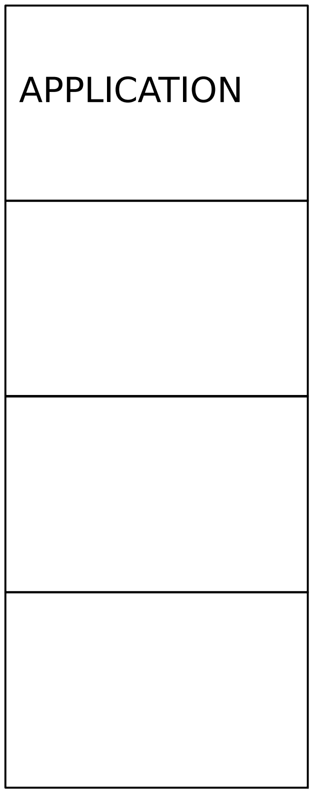
HARDWARE ADDRESS

MAC ADDRESS

ETHERNET ADDRESS



Application Layer



HIGHEST LAYER

ONLY LAYER VISIBLE TO USERS

INTERACTS WITH TRANSPORT LAYER

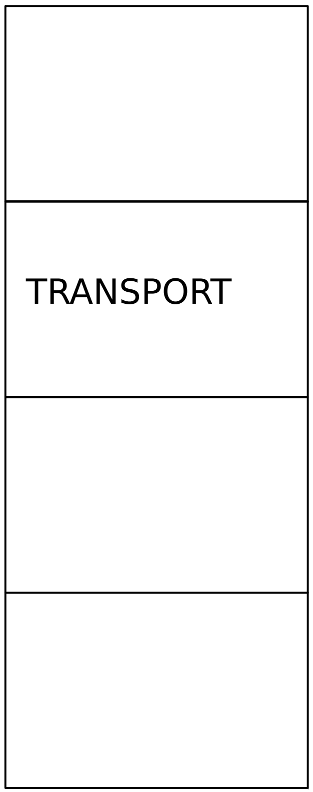
DECIDES WHICH TRANSPORT PROTOCOL TO USE

COMMONLY KNOWN PROCESSES

- TELNET
- FTP
- SMTP
- DNS
- RIP
- WWW

Transport Layer

MSTP



RESPONSIBLE FOR HOST TO HOST DATA TRANSMISSION

KEEPS TRACK OF DATA RECEPTION & PASSES DATA TO APPLICATION ITSELF - TWO PROTOCOLS ARE :

TCP
- RELIABLE
- ACKNOWLEDGMENT
- REGULATES DATA FLOW
- ERROR DETECTION AND CORRECTION

UDP
- UNRELIABLE
- RELIES ON UPPER LAYERS FOR ERROR DETECTION
- LOWER OVERHEAD

Internet Layer

MSTP

Internet

Provides basic packet delivery

Routing decisions

Encapsulates packet in datagram

Fragmentation and reassembly of packets

Connectionless

Unreliable

Interface Layer

MSTP

**NETWOR
K**
INTERFACE

- Accepts datagrams and transmits over media
- Node to node over single link
- Must know underlying transmission protocol
- One protocol for every network access protocol
- Data integrity
- Computes and checks checksums
- Encapsulation of datagrams
- Maps network addresses to hardware addresses
    - **ARP**
    - **RARP**

Network Interface Layer Addressing

MSTP

- Hardware address
- MAC address
- Ethernet address
- 48 bits
- 05 23 33 20 00 f4
- 2 portions
  - Vendor code
    - First 6 characters
    - Assigned by IEEE
  - Unique hardware address
    - Last 6 characters
    - Assigned by vendor
- Actual address to which frames are sent

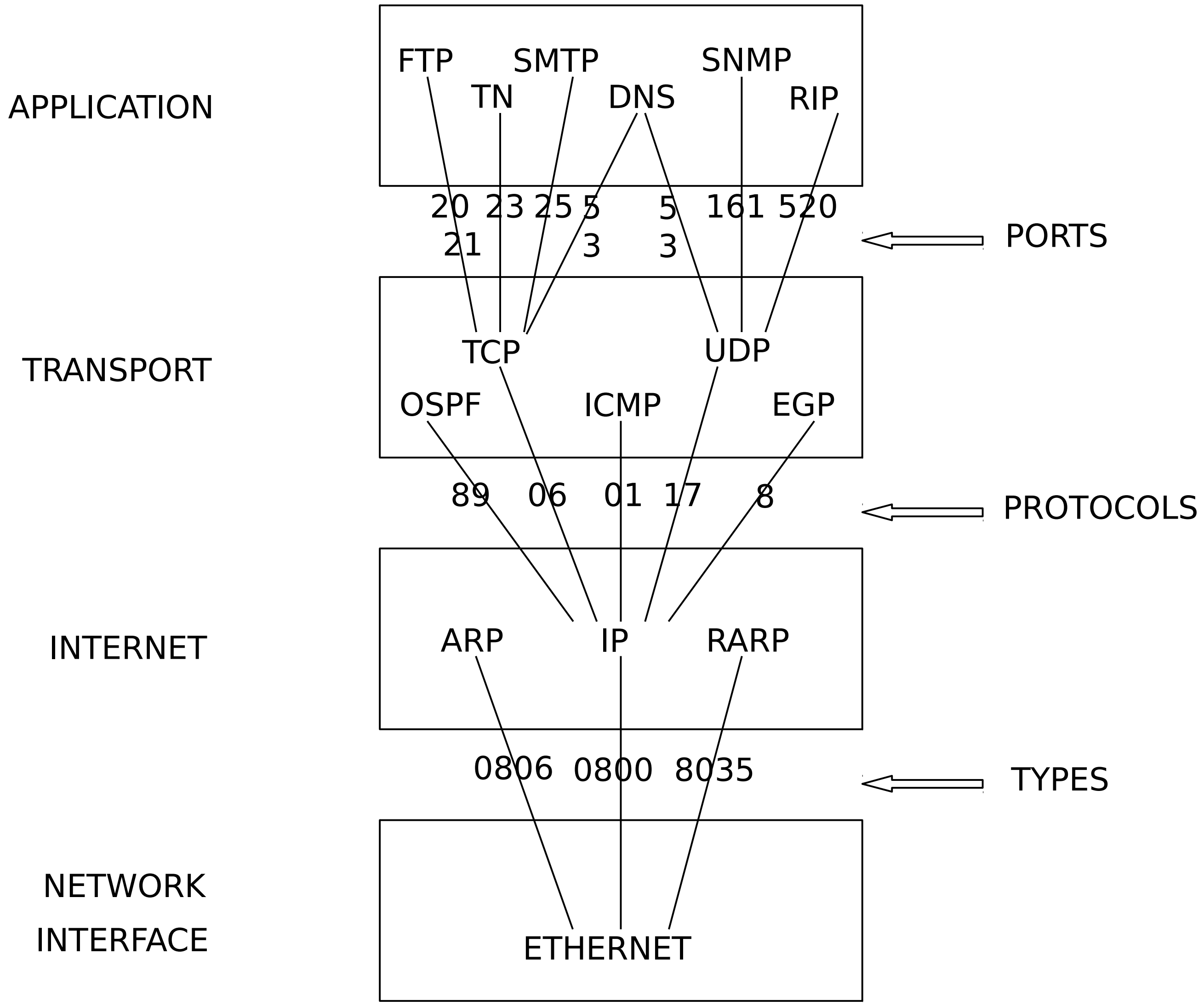
Network Interface Card

MSTP

- Network Interface Card (NIC) listens for:
  - It's hardware address
  - Broadcast address
  - Multicast address
- Decision Process
  - Ethernet NIC
    - Mine - Pass it to internet layer
    - Not Mine - Discard
  - Token Ring NIC
    - Mine - Pass it to internet layer
    - Not Mine - Regenerate and pass along

Inter-layer Communication

MSTP



Request for Comments (RFC)

- The internet explains the open standard that makes up TCP/IP and related Internet protocols in Request for Comments (RFC's)

- RFC's are also written on many networking topics. Each new and received/replacement RFC is assigned a sequential number in the order that they are submitted.

Address Resolution Protocol (ARP)

- RFC 826
- Converts network address to hardware address
  - Deliver data from one host to another on same network
- Supported by majority of vendor's implementations
- Sender knows network address but not hardware address
  - Sender broadcasts ARP request to all hosts
  - All interfaces receive ARP request
    - If not mine, drop
    - If mine, reply to send
  - Sender caches hardware and network address
  - Sender sends data to recipient

Reverse Address Resolution Protocol (RARP)

- RFC 903 / 906
- Maps hardware addresses to network addresses
- Allows diskless clients to learn their own network addresses
- Workstation knows hardware address but not network address
  - Workstation broadcasts RARP request onto network
  - RARP server responds with network address
- Special chipset on NIC required
- RARP server must be available and

IP Addressing & Classes

Table of Contents

MSTP

- Binary Numbering
- Binary to Decimal
- IP Addressing
- Subnetting
- Questions
- Summarization

Binary Numbering

MSTP

- Computer works using the binary numbering system.
- Recognizes two states, the ***presence*** of an electrical charge or the ***absence*** of an electrical charge. In other words, **on or off.**
- Binary numbering system is ideal for representing these two states
  - Consists of only two digits. (smallest – largest) 0 and 1
  - 0 represents the absence of an electrical charge or 'off'.
    1 represents the presence of an electrical charge or 'on'.

- **Bit = 1 digit (one or a zero)**
- **Byte = 8 bits**
- **Octet = Always 8 bits**

Binary To Decimal

MSTP

ONE OCTET CAN BE BROKEN DOWN INTO

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

2=2
2x2=4
2x2x2=8
2x2x2x2=16
2x2x2x2x2=32
2x2x2x2x2x2=64
2x2x2x2x2x2x2=128

Binary to Decimal Conversion

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1
0	1	0	1	0	1	0	1

- 128 64 32 16 8 4 2 1
- 0 0 0 0 0 0 0 0
  00000000 = 0
- 1 1 1 1 1 1 1 1
  11111111 = 255
- 0 0 0 0 1 1 1 1
  00001111 = 15
- 0 1 0 1 0 1 0 1
  01010101 = 85

Binary (Cont.)

MSTP

- 00000000 = 0
- 10000000 = 128
- 11000000 = 192
- 11100000 = 224
- 11110000 = 240
- 11111000 = 248
- 11111100 = 252
- 11111110 = 254
- 11111111 = 255

IP Addressing

MSTP

- 32 BITS - 4 BYTES –
- MUST BE UNIQUE FOR EACH HOST IN NETWORK (8 BITS = 1 BYTE)
  - 192.168.20.10
  - 192.168.31.33

- 2 [3] PORTIONS

  Network portion – Relative to the class of IP. Identifies the network and is common to all devices attached to that network.

  Host portion - also relative to class as well as identifies a particular device attached to that network.

  [Subnet portion]

Net ID	Host ID	
Net ID	Subnet ID	Host ID

Addressing/Classes

MSTP

- xxx.xxx.xxx.xxx **n =network h=host address**
  - **192.156.2.169 (IPv4)**

- **Class A** nnn.hhh.hhh.hhh **1 - 126**
  - Only 126 networks, but 16,777,214 hosts apiece
    - **127.0.0.1 = Local loop back address**
- **Class B** nnn.nnn.hhh.hhh **128 - 191**
  - 16,384 networks with 65,534 hosts apiece
- **Class C** nnn.nnn.nnn.hhh **192 - 223**
  - 2,097,152 networks with 254 hosts apiece
- **Class D - used for multicasting (audio/video)**
- **Class E - currently reserved / future**

Class Conversion

MSTP

128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1

Rule

A MIN **0** 0 0 0 0 0 0 0

MAX **0** 1 1 1 1 1 1 1

(2^24-2) = 16,777,214

-2 for broadcast and network

2^7-2 = 126 networks

Decimal Range **1-126**

0 and 127 are reserved

B **1** **0** 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

1 **0** 1 1 1 1 1 1. 0 0 0 0 0 0 0 0

2^16-2 = 65,524 hosts per network

2^14 = 16,384 networks

Decimal Range 128-191

C **1** **1** **0** 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

1 **1** **0** 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

2^21 = 2,097,152 networks

2^8-2 =254 host per network

Decimal to Binary Example

MSTP

192.156.69.0 =
11000000.10011100.01000101.00000000

Class C

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

128+64 = 192

128	64	32	16	8	4	2	1
1	0	0	1	1	1	0	0

128+16+8+4 = 156

128	64	32	16	8	4	2	1
0	1	0	0	0	1	0	1

64+4+1 = 69

Let Practice!!

Reserved IP Addresses

MSTP

- IP address for Hosts cannot have:

  ALL 1's or ALL 0's (binary) in the NETWORK portion
  OR
  ALL 1's or ALL 0's (binary) in the HOST portion

  - All 1’s in the host portion of a target IP address signifies a Broadcast
  - All 0’s in the host portion of a IP address identify a subnet or network

- Network: 138.156.0.0 = 10001010.10011110.00000000.00000000
  Broadcast:138.156.255.255 = 10001010.10011110.11111111.11111111
  Host: 138.156.100.100 = 10001010.10011110.01100100.01100100

IP Addresses

- ASSIGNED by Node Site Coordinator
  - Address assignment planning
  - Node Site Coordinator
  - Draw out your network
  - Same "physical" net means same ”IP Network”
  - Each "interface" has a "unique" IP address
  - “Don't" assign reserved addresses

- RECOMMENDATIONS
  - FIRST 10 addresses reserved for router interfaces
  - LAST address reserved for domain name

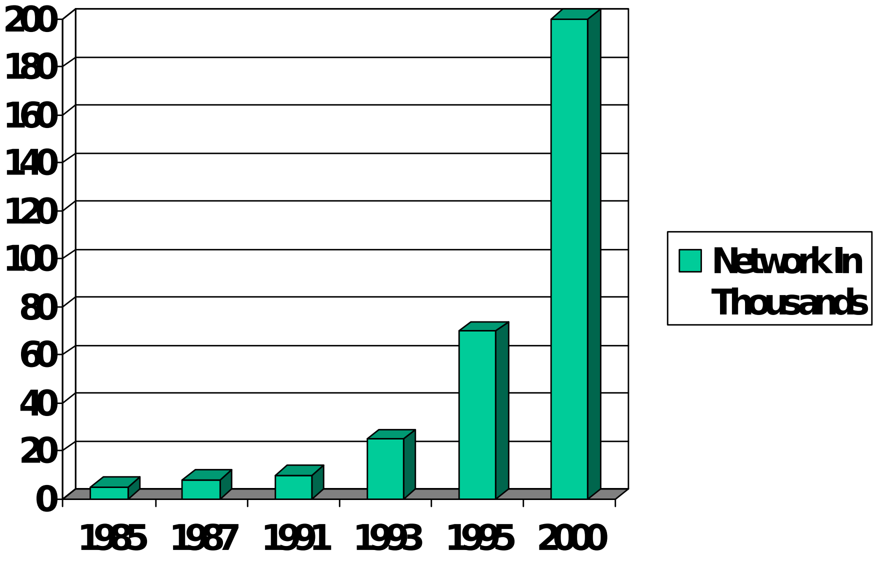
TCP/IP

SUBNETTING

A little History to Why We Subnet

MSTP

- The growth of the Internet
- Depletion of IP Addresses – currently we have IPv4 which gives us 4,294,967,296 IP Address. (2^32)
- Administrator where not meeting current requirements based on the two-level classful IP address. Classful address were not be allocated efficiently.
- Growth caused Internet router's routing tables to increase



Terminology

MSTP

- Address Mask – All network bits set to 1 and all host bits set to 0
- Subnet - A subnetwork of a major class A, B, C address space
- Subnet Mask - A mask longer than the standard address mask - determined by subnet scheme.

IP Address Terminology

MSTP

- **NETWORK NUMBER**- When all host bits are turned off (0).
- **BROADCAST ADDRESS**- When all host bits are turned on (1).
- **HOST ADDRESS**- A unique IP address assigned to a workstation, interface or user, that is in between the network number and broadcast address.
- **SUBNET MASK**-Used to tell the machine what subnetting scheme is being implemented on the network. Found by turning all network bits on (1), including those host bits that have been given to the network side.
- **SUBNETTING** - Dividing up an entire Class network by sacrificing original host (H) bits to the network (N).

SUBNETTING

MSTP

- WHAT IS IT?
  Divides host (H) portion into smaller networks
- WHY?
  Stops wasting network numbers
- WHO?
  Node site coordinator
- WHAT DETERMINES?
  Number of different physical networks and number of hosts

Subnetting

MSTP

- When you borrow bits from the main network address's host section, TCP/IP must be told which bits of the host section are borrowed to be used as the network address.

- We use a subnet mask to define the number of bits used to create additional networks.

- **Remember** - the more bits used

Default Subnet Mask

Your network has a subnet mask even if it doesn't have

CLASS A DEFALUT = 255.0.0.0

11111111.00000000.00000000.000000

CLASS B DEFAULT = 255.255.0.0

11111111.11111111.00000000.000000

CLASS C DEFAULT = 255.255.255.0

11111111.11111111.11111111.000000

Class Conversion

MSTP

128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1. 128 64 32 16 8 4 2 1

Rule

A MIN **0** 0 0 0 0 0 0 0

MAX **0** 1 1 1 1 1 1 1

(2^24-2) = 16,777,214

-2 for broadcast and network

2^7-2 = 126 networks

Decimal Range **1-126**

0 and 127 are reserved

B **1** **0** 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

1 **0** 1 1 1 1 1 1. 0 0 0 0 0 0 0 0

2^16-2 = 65,524 hosts per network

2^14 = 16,384 networks

Decimal Range 128-191

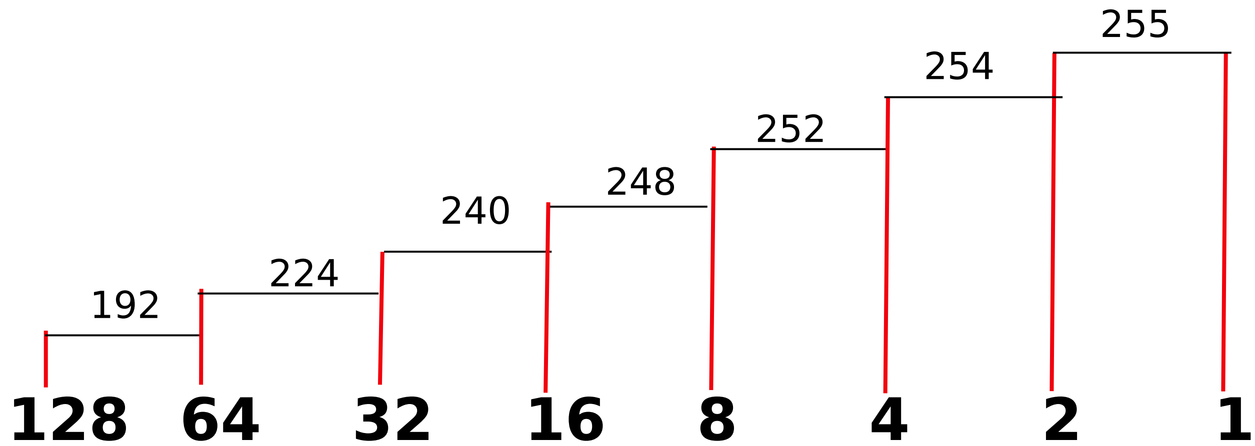
C **1** **1** **0** 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

1 **1** **0** 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

2^21 = 2,097,152 networks

2^8-2 =254 host per network

Subnet Bit Chart



* SUBNET BITS COME FROM THE HIGHEST-ORDER BITS TO THE LOW ORDER BITS OF THE **HOST** FIELD

How Subnetting Works

MSTP

16 -(2) # hosts per network
- all 0's network
- all 1's broadcast

leaves 14 per net

N				H			
128	64	32	16	8	4	2	1

MASK = 128+64+32+16
240

N				H				
128	64	32	16	8	4	2	1	
0	0	0	1	0	0	0	0	16 Network
0	0	0	1	0	0	0	1	17 1st host
0	0	0	1	0	0	1	0	18
0	0	0	1	0	0	1	1	19
:	:	:	:	:	:	:	:	
0	0	0	1	1	1	1	1	31
Broadcast								
0	0	1	0	0	0	0	0	32

Determining Subnet Mask

MSTP

N H

192.156.69.0= 11000000.10011100.01000101.00000000   Class C

N.N.N.H

N H

143.211.0.0 = 10001111.11010011.00000000.00000000   Class B

N.N.H.H

Subnet Mask is the address with every network bit turned on. This tells the
router that you want to use some Host bits as network (subnet) bits.

N H

192.156.69.0= 11000000.10011100.01000101.00000000   Class C

N.N.N.H

Subnet Mask= 11111111.11111111.11111111.00000000   255.255.255.0

N H

with 4 bit   = 11111111.11111111.11111111.11110000

255.255.255.240

N H

143.211.0.0 = 10001111.11010011.00000000.00000000   Class B

N.N.H.H

Subnet Mask= 11111111.11111111.00000000.00000000   255.255.0.0

N H

with 8 bit   = 11111111.11111111.11111111.0000000

Subnetting Reference Charts

MSTP

CLASS B

# BITS	SUBNET MASK	# SUBNETS	# HOSTS
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Subnetting Reference Charts

MSTP

CLASS C

# BITS	SUBNET MASK	# SUBNETS	# HOSTS
2	255.255.255.192	4	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Steps in Subnetting

MSTP

1. Write Out the Subnet Mask
2. Answer What You Know
3. Write Out in Binary
4. Apply Logical And (or Anding)
5. Turn on all the host bits

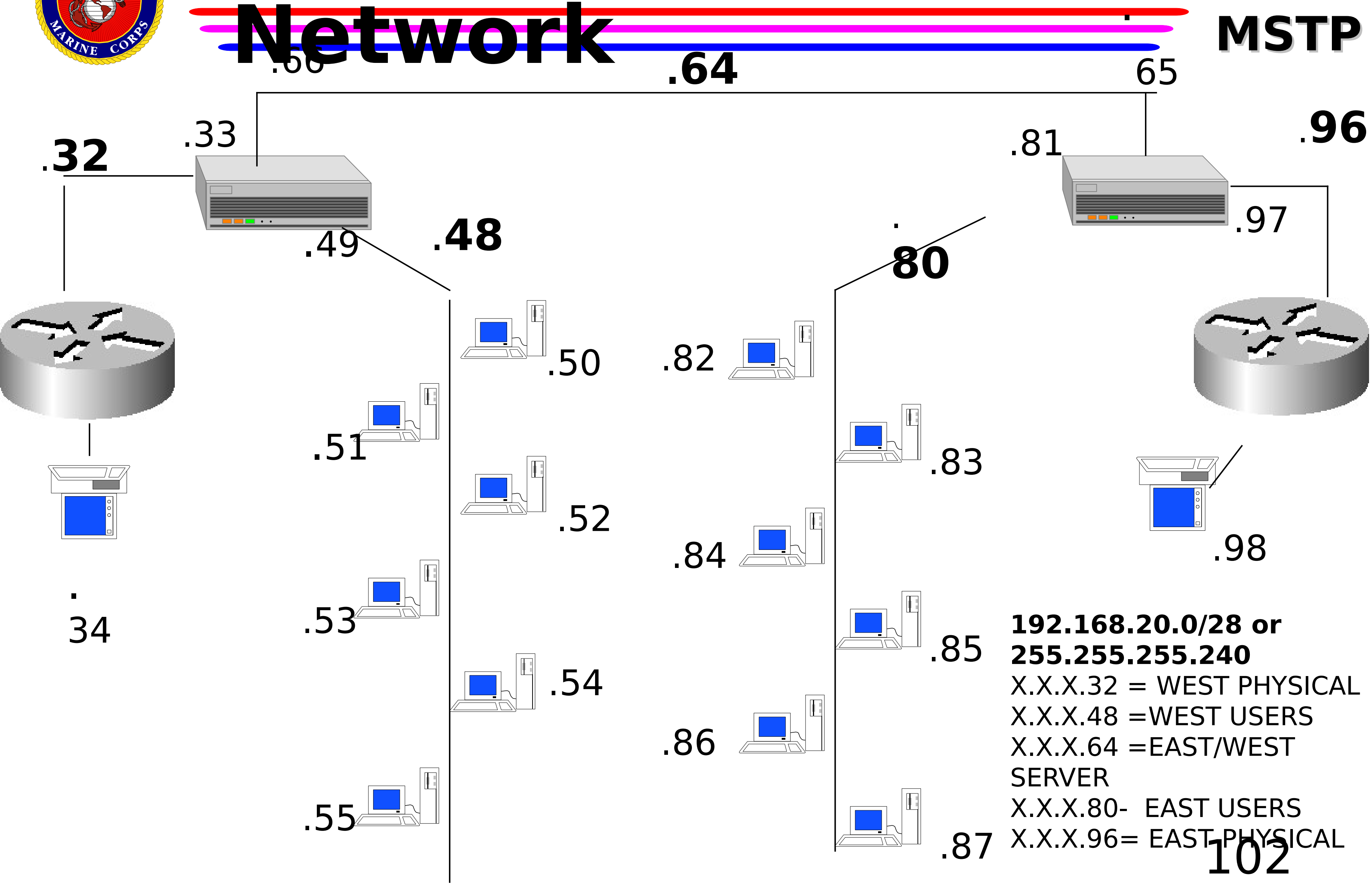
192.168.25.45 / 27

192.168.25.45
255.255.255.224
192.168.25.??

128 64 32 16 8 4 2 1
1 1 1 0 0 0 0 0
0 0 1 0 1 1 0 1
0 0 1 0 0 0 0 0
0 0 1 **1** 1 1 1 1

101

Sample Subnetted Network



192.168.20.0/28 or
255.255.255.240
X.X.X.32 = WEST PHYSICAL
X.X.X.48 =WEST USERS
X.X.X.64 =EAST/WEST SERVER
X.X.X.80- EAST USERS
X.X.X.96= EAST PHYSICAL

Going Beyond The Octet

MSTP

N | H

10 Bit
1022 Nets
62 Hosts

32768	16384	8192	4096	2048	1024	512	256									
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0.64 Network
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0.65 1st host
0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0.66 2nd Host
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0.127 Broadcast
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0.128 Network
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0.129 1st host

6 Bit
62 Nets
1022 Hosts

32768	16384	8192	4096	2048	1024	512	256									
128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4.0 Network
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	4.1 1st host
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	7.255 Broadcast
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	8.0 Network

Finding A Host's Network

MSTP

N H

Host: 192.156.69.78 = 11000000.10011100.01000101.0100 1110

Subnet Mask 4 bit = 11111111.11111111.11111111.1111 0000

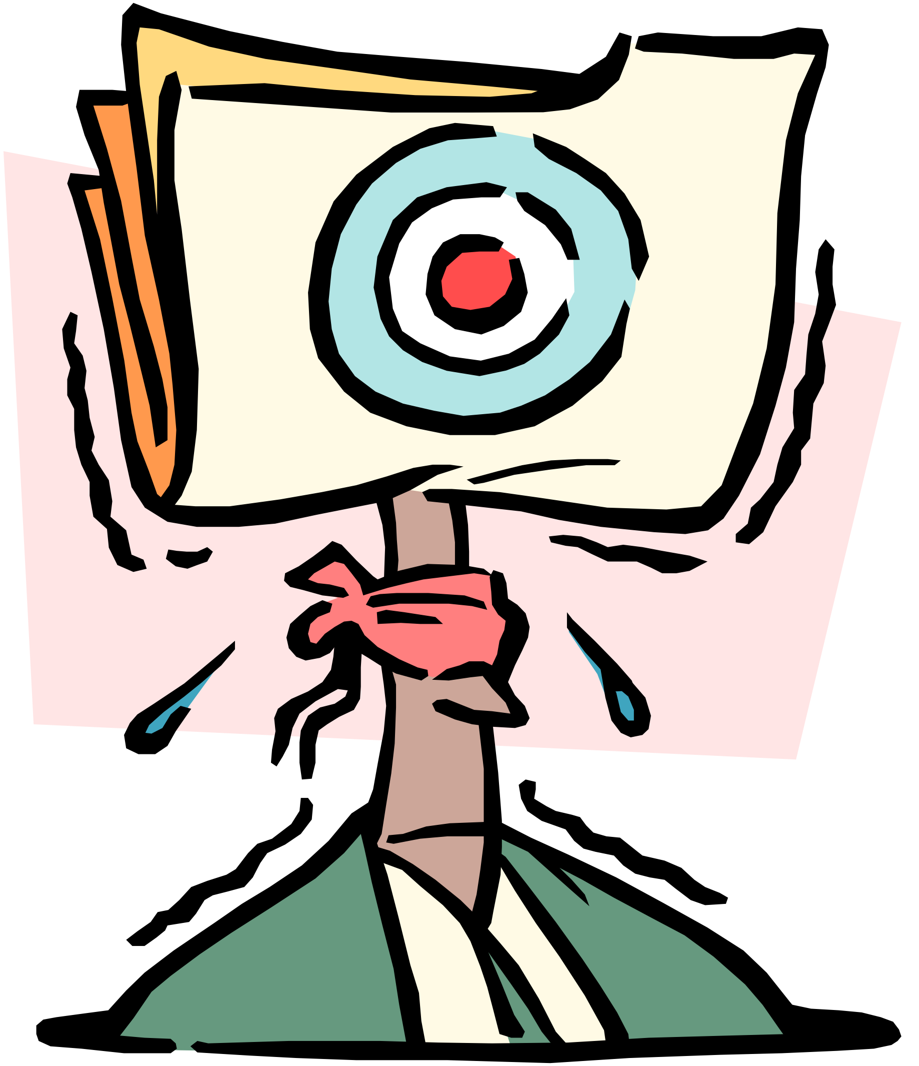
Host Network ID # = 11000000.10011100.01000101.0100 0000

Network bits total 192.156.69.64
which is not all 1's or all 0's.

Host bits = 1110 which is not all 1's or all 0's so it is legal, it is the
14th host on the .64 network.

Is there another way?

MSTP



Five Questions

MSTP

- 1. How many subnets?
- 2. How many hosts per subnet?
- 3. What are the subnets?
- 4. What are the valid hosts in each subnet?
- 5. What is the broadcast address of each subnet?

Begin to answer by…

MSTP

1. Determine how many networks you need.
2. Find out how many hosts are required for each network (use the highest number of hosts).
3. Choose the subnetting scheme that will best support all networks (leave room for growth).
4. Assign network numbers.
5. Assign unique addresses to

Five Answers

MSTP

- 1. 2^n = Amount of subnets.
- 2. $2^n - 2$ = Amount of hosts per subnet.
- 3. 256 – Subnet mask = Base number.
- 4. Valid hosts are the numbers between the subnets, minus all 0’s and all 1’s.
- 5. Broadcast address is all 1’s or the number before the next subnet.

Prefix Routing

MSTP

- Means by which the Internet identifies the portion of the 32-bit TCP/IP address
  - /27 255.255.255.224
  - /26 255.255.255.192
  - /25 255.255.255.128
  - /24 255.255.255.0
  - /23 255.255.254.0

Discontiguous Addressing

- Two networks of the same classful networks are separated by a different network address.
- When using RIP or IGRP, you must use the default-router command.

Summarization

MSTP

- Allows contiguous networks to be grouped together and advertised as one large network
- Also known as supernetting

Any Questions

MSTP